MUTUALLY ASSURED DELETION:
THE UNCERTAIN FUTURE OF MASS DESTRUCTION IN CYBERSPACE

BY

MAJ NATHANIEL R. HUSTON

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUN 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **Mutually Assured Deletion: The Uncertain Future Of Mass Destruction In Cyberspace**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School Of Advanced Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Much like air power in the early 20th Century, cyber operations offer a new context within which to consider the nature and character of war. Given the fledgling nature of the domain and the intrinsic rapidity with which it expands, contemplating its role in future conflict becomes increasingly important, especially as it proliferates ever deeper into both civil and military systems. While cyber advocates have begun the early stages of this examination, the surface has barely been scratched and the body of work appears to reflect an undercurrent of anxiety bordering on panic regarding what is judged to be a public and bureaucratic indifference to the threat posed by cyber vulnerabilities. The tendency to focus on these vulnerabilities and threats constitutes an uneven and overly constricted view of the problem. In a post-Cold War age characterized by uncertainty and perhaps even multi-polarity, the need to take a balanced and objective view of the future of cyber is increasingly pronounced.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**109**	

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

SUZANNE C. BUONO (Date)

MELVIN G. DEAILE (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Nate Huston entered the Air Force through the Reserve Officer Training Corps and earned his bachelor's degree in Computer Engineering at the University of Notre Dame in 1999. After commissioning, Major Huston spent time in the missile fields of Montana at Malmstrom Air Force Base, followed by a hardship tour supporting the PACOM J2 stationed at Pearl Harbor, Hawaii. Upon his return to the continental United States, Major Huston spent the best four years of his career in various positions at the 5th Combat Communications Group while stationed at Robins Air Force Base, Georgia, after which he did penance in Air Combat Command's A5 directorate as an Intelligence, Surveillance, and Reconnaissance as well as Command and Control programmer. In addition to his bachelor's degree, Major Huston holds a Master's of Military Art and Science from Air Command and Staff College.

ACKNOWLEDGEMENTS

I would first like to thank the Deuces of Class XXII for their inspirational and irrepressible spirit, without which none of this year would have been possible, due to what I am confident would have been multiple aneurisms. In particular, I would like to thank the men and woman of the H-K kennels. Their constant humor and unequaled drive has truly been a perpetual source of encouragement throughout this grueling year. I am confident there will never be another group quite like that formed by the likes of Razorblades, Jay, Chode, Chili, Scab, Chantel, Freud, and Chief. I must also thank Maj Brian "Brutus" Stahl for his wise words, which inspired the title to this thesis. I suppose I must admit that his calculations were correct: he really *is* one of the most awesome Raptor pilots ever. Thanks to the faculty and staff of SAASS, especially Ms. Sheila, Ms. Kelly, and each of my instructors, for their patience and intellect. A special thanks to Colonel Suzanne Buono, for her tireless determination to improve my oft-tangled prose, her vigorous comma correction, unparalleled citation enforcement, and, above all else, her indefatigable and resolute efforts, unchecked by time constraints, to fortify my ideas and guide me through the darkness of thesis creation. I would also like to thank Dr. Jim Forsyth, whose personal tranquility and intellectual fortitude was a constant source of strength and without whom, I would doubtless still be searching for a topic. Many thanks to Colonel Melvin Deaile, whom I am confident found this thesis delightful and in need of no major corrections.

Finally, and most importantly, I must thank the most important and without doubt most critical contributors to this thesis: The Huston Team. To my wife I owe every good thing that has ever happened to me. Your love and strength has always been the guiding light for our family, and this year was no exception. I must thank our beautiful little girls for their constant levity and understanding as I buried my nose in books and hacked away at the computer morning, noon, and night. Each of you inspires me every day. Everything I do is for our team. I hope to one day repay your for your unconditional love and support throughout this year.

ABSTRACT

Much like air power in the early 20th Century, cyber operations offer a new context within which to consider the nature and character of war. Given the fledgling nature of the domain and the intrinsic rapidity with which it expands, contemplating its role in future conflict becomes increasingly important, especially as it proliferates ever deeper into both civil and military systems. While cyber advocates have begun the early stages of this examination, the surface has barely been scratched and the body of work appears to reflect an undercurrent of anxiety bordering on panic regarding what is judged to be a public and bureaucratic indifference to the threat posed by cyber vulnerabilities. The tendency to focus on these vulnerabilities and threats constitutes an uneven and overly constricted view of the problem. In a post-Cold War age characterized by uncertainty and perhaps even multi-polarity, the need to take a balanced and objective view of the future of cyber is increasingly pronounced.

This thesis posits that a prevailing tenor of technological determinism vis-à-vis cyberspace and its relationship with international security may have crowded out more nuanced analysis of its future role in the geopolitical landscape. In order to discern the prospects for a less dystopian future, it examines the histories of three separate classes of weapons: landmines, chemical and biological weapons, and nuclear weapons. While each is unique, and the reasoning for their limitation varied, the conglomeration of all three is shown to exhibit a powerful trend; namely, that the ability to destroy or kill does not necessarily translate into the fullest expression of that capacity. In light of this historical precedent, the final section examines some of the underlying causes for the predominantly pessimistic view of the future and suggests that though warfare by, with, and through cyberspace may indeed devolve into indiscriminate attacks on civilian populations, history reflects a potential for restraint. There is no invisible force propelling weapons toward greater and greater destruction and no predetermined path toward increased adverse effects on civilians, even in the world of cyberspace.

CONTENTS

INTRODUCTION

As the world explores the new realm of cyberspace and cyber power, it appears to have settled on a conventional perspective regarding their use in future warfare. The specter of mass chaos via power grid failures, dams bursting and financial turmoil looms large over an increasing number of cyber discussions. Many of today's cyber scholars appear to believe that this new capability offers the prospect of mass destruction and that, given the right circumstances, man will exploit it. Warfare by, with, and through cyberspace promises to touch more lives, affect more people, disrupt more systems, than ever before in the history of the world. But will it?

A consensus exists that predicts that the introduction of cyber operations will disregard an international norm that eschews wanton violence against a civilian populace. Many advocate a decidedly determinist outlook that conflict in cyberspace will increasingly turn away from precision and instead usher in an era of greater and more widespread destruction. How realistic is this notion? Does warfare promise an increase in mass destruction, of cyber-induced pandemonium? Conventional wisdom regarding cyberspace is too narrowly focused on the increased potential for widespread rapid destruction and, furthermore, pays virtually no heed to the other aspect of its dual nature: its potential for hyper-precision.[1] It predicts that mankind will take the path of increased capability against growing vulnerability and increasingly target the civilian populace of an adversary. Many argue that inevitably, existence of the capability will itself drive its own employment against the entire population of the state. The efficacy of such a strategy notwithstanding, the certainty with which this future is envisioned is

[1] I use the term "hyper-precision," expanded upon in chapter 3, to refer to the exponential increase in precision offered through the exploitation of cyberspace. Instead of needing to demolish a building (or even a portion of a building) in order to disable electronic equipment inside of it, cyberspace offers the ability to target the equipment itself, or even one small portion of it (assuming, of course, there is an electronic path to it, though even so-called air gaps can be jumped via human intervention), oftentimes with little to no physical or collateral damage. This aspect of operations in cyberspace is particularly well articulated in a paper presented by Robert Fanelli and Gregory Conti to the fourth International Conference on Cyber Conflict. They show that the effects of cyber actions can be constrained "to specifically desired, legitimate targets while significantly limiting collateral damage and injury to non-combatants." Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict" (paper presented at the 4th International Conference on Cyber Conflict 2012), 319. Non-kinetic targeting of electronic equipment through cyberspace can in some instances deliver the same effects heretofore only achievable through kinetic destruction. Cyberspace offers a granularity that is orders of magnitude greater than traditional kinetic weapons, hence the term "hyper-precision."

questionable.[2] It is overly deterministic, appears to wholly discount any sociological pressures on the employment of technology, and paints an overly simplistic future derived from a fallacious notion of the technology itself as causal. Furthermore, the argument generally ignores examples of similar innovation from the recent past that induced comparable fears; yet, that ultimately resulted in constraint, even during some of the most brutal and widespread wars in history. The undercurrent of impending hysteria in today's cyber literature reflects an oversimplification of what is in reality a very complex and wide-ranging subject: technology in war. Of all of mankind's creations, war may be its most impenetrable. Its complexity is at once beautiful and horrific. Those who contend that warfare within the cyberspace domain is somehow reducible to a "we can, therefore we will" argument drastically underestimate the matter.

There is no arguing that the "information revolution" has fundamentally altered the way the world operates. Systems and societies are increasingly networked together and while these connections offer vulnerabilities, they also offer the potential for precision heretofore unimagined in warfare. Contemporary cyber thinkers have explored deeply the vulnerabilities introduced by the information revolution but have largely ignored cyberspace's more important impact: its potential for precision and what that suggests about its future exploitation and use. Advocates of the cyber pandemonium school of thought predict an "If we can, we will" strategy[3] vis-à-vis cyberspace's potential for destruction but largely discount the increased ability to target increasingly discrete objectives.

As war's character has mutated and shifted, it has followed a continuous trend toward greater discrimination. Where the potential for precision has been introduced, it has been embraced. Use of weapons that lack discrimination has generally been

[2] Robert Pape argues in *Bombing to Win: Air Power and Coercion in War* that attempted coercion through targeting of a civilian populace is nearly guaranteed to fail. He contends that a century's worth of attempts to do so via air power have proven ineffective. Ultimately, he suggests that a strategy of denial of the adversary's aims, rather than one of coercion through punishment, is most likely to prove successful. In any case, air power strategies since the early twentieth century offer a plethora of case studies that cast at least some doubt on the notion of a population-centric approach to warfare. Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 315-17, 26.

[3] Chapter 1 will identify specific proponents of this position and explore their position in depth.

avoided.[4] While there are outliers, an historically consistent trend toward the adoptions of maximal discrimination in the conduct of warfare is nonetheless identifiable. To the extent that the trend can be illustrated, how does the introduction of operations by, with and through cyberspace affect it? Will cyberspace's potential for widespread destruction tend to reverse the international march toward discrimination, or will its potential for hyper-precision win the day and propel warfare even further down the path toward discrimination? Will the forces that have historically pushed the trend toward precision suffice to reign in the destructive potential of cyber-weaponry, or is there some fundamental difference in the nature of cyberspace that will enable it to resist these forces and reverse the trend? Will cyber follow the trend of previous weapons toward greater and greater precision or will it go the other way, toward greater destruction and mass hysteria? Contrary to popular belief, these issues are anything but decided.

Is Mankind's Fate Sealed?

Twenty years ago, as the internet was just beginning its rise to information prominence, the risk associated with connectivity was only fully comprehended by a few experts in the still-emerging field. As connectivity wove its way ever deeper into civilian and especially military systems, those experts found themselves nearly screaming to have their voices heard above the din of excitement over increased convenience and capability.[5] In seeking to convey the gravity of the challenge, they may have swung the pendulum too far in the other direction. The tenor of cyber scholarship today reflects a

[4] Note that this refers specifically to war, as separate from terrorism, a distinction that is addressed in greater detail below.

[5] The challenge of educating the government and the public regarding the vulnerabilities introduced during the boom of connectivity witnessed in the 1990s and early 2000s was foreboding. Alan Campen, one-time manager of the Armed Forces Communications and Electronics Association, alluded to this difficulty in the preface to *Cyberwar*, written in 1996. In it, he highlighted the dangers of rapidly digitized and interconnected "functions of human enterprise…stored and processed within information systems having only the most rudimentary safeguards against disruption or manipulation…." Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, *Cyberwar: Security, Strategy, and Conflict in the Information Age* (Fairfax, VA: AFCEA International Press, 1996), vii. The frustration facing computer security professionals is at the center of Mark Bowden's *Worm,* where the central protagonists, those who make up the so-called "Tribe" of security experts, face constant challenges when trying to educate governmental and commercial leadership as well as the general public as to the vulnerabilities associated with the Internet and its interaction with a country's vital modern infrastructure. Ultimately, the "wall of incomprehension and disbelief" they face becomes even more problematic due to the number of false alarms that have been sounded in the past. They face a "boy who cried wolf" problem of attempting to educate the public as to the real dangers associated with cyberspace while at the same time attempting to remain realistic as the probability of their manifestation. Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011), 24-25.

strong tendency toward technological determinism, the momentum of technology propelling itself forward along a path of advancement that ultimately cannot be contained by mere human desires.[6] The logic is tempting. "[T]he thingness or tangibility of mechanical devices…helps to create a sense of causal efficacy made visible."[7] One author goes so far as to suggest that not only is technological development sequential and continuous, its future is even predictable and "imposes a determinate pattern of social relations on [a given] society."[8]

The world of technical innovation, however, especially in cyberspace, is not nearly so straightforward. Instead, the path of innovation is full of failed initiatives, suspicious and skeptical bureaucrats, cost overruns, and innumerable other twists, forks, and dead-ends. This is not to say that the social constructivists have cornered the cyber market either. The innovation of information delivery and manipulation enabled through the growth of cyberspace transcends the model of artifact as conceived as solution to a socially defined dilemma.[9] It seems clear that cyberspace will not be bent to any singular will. Rather, cyberspace finds itself somewhere in between. The discussion of technological determinism versus social constructivism, especially with regard to cyberspace, is a false dichotomy. Development and innovation in cyberspace exist along a spectrum and within a system of actors, each of which shapes and molds the future of the technology and those who wield it. This is important in light of the overwhelming inevitability that characterizes much of today's cyberspace dialogue. Determinism is attractive because "it creates powerful scenarios, clear stories, and because it accords with the dominant experience in the West." [10] These scenarios and stories, however, may oversimplify what is at its core a set of very complex and challenging issues. At the very least, they de-emphasize the power of societies and international norms to constrain behavior and, in so doing, risk conflating possibility and inevitability.

[6] This sort of logic permeates much of the contemporary writing regarding conflict in cyberspace. It is examined in depth in Chapter 1.

[7] Merritt Roe Smith and Leo Marx, *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994), xi.

[8] Smith and Marx, *Does Technology Drive History?*, 56-57, 59.

[9] Wiebe E. Bijker, Thomas Parke Hughes, and T. J. Pinch, *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987), 33-36.

[10] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), 289.

Whether conflict in cyberspace will ultimately devolve into the cataclysm predicted by many of today's scholars cannot be known definitively. However, in taking such a determinist view of the future, the community risks blinding itself to other possibilities and, worse, inducing that which it would appear to warn against. Alexander Wendt, a renowned political scientist, argues that, in the context of international relations, culture can be a self-fulfilling prophesy. Faced with a situation in which one must interact, an actor must define the situation before choosing a course of action. The actor's definition will be based on both his own identity as well as how he expects others to act. The need to define the situation necessarily leads to an individual construction of reality.[11] In attempting to underline the risk associated with a growing reliance on connectivity, experts are at risk of constructing a culture of alarm and hypersensitivity blind to the prospects of an alternative future and one that predisposes decision-makers to be constantly on guard for the cyber-bogeyman lurking in the shadows. Man has a strong tendency to see what he expects to see and to assimilate information into pre-existing images. While this behavior is rational and even necessary, it can result in missing or dismissing information that does not fit the pre-determined model.[12]

This research attempts to more fully elucidate the current environment of cyberspace and ascertain just how locked in its future is. It first reviews current literature in order to illuminate the undercurrent of hyperbole and hysteria surrounding the future of conflict in cyberspace. Next, it surveys three similar cases of the introduction of new technology into warfare and examines contemporary predictions of their effects on warfare as well as their ultimate proliferation or constraint. Finally, cyberspace is examined in-depth in order to determine what drives the prevailing outlook and attempt to establish a plausible alternative. Before proceeding, it is necessary to bound the discussion.

Setting the Stage

As has already been alluded to, cyberspace is still new. Its boundaries are not well-defined, terms are not agreed upon, even its nature as a warfighting domain is hotly

[11] Alexander Wendt, *Social Theory of International Politics*, Cambridge Studies in International Relations (New York: Cambridge University Press, 1999), 186.
[12] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 117, 43-45.

debated. Too often, disagreements over definitions tend to sidetrack more useful discussions and prevent exploration of more salient issues. At worst, this risks argument by definition.[13] In order to avoid being overcome by semantic deliberation, this research relies on a broad definition that, though admittedly debatable, will allow for a more in-depth discussion of the impacts of operations in cyberspace. "For argument's sake" evokes the tone and intent of the following discussion.

Defining the Stage

In order to sew confusion, one needs only to append the word "cyber" to the front of any otherwise clearly understood term or phrase. This is true even of the foundational term "cyberspace." Its origin can be traced to William Gibson's 1984 science fiction novel, *Neuromancer*, but its meaning defies consensus 30 years later.[14] In some contexts, it can be useful to define cyberspace through spotlighting its most salient characteristic, as in "cyberspace is about networking, the two-way transfer of information, in contrast to broadcasting, in which information is transferred only one way."[15] In other cases, it may be more useful to define it functionally and spatially. One author, for example, defines "cyberspace" as "the domain in which cyber operations take place" as opposed to "cyber power," which "is the sum of strategic effects generated by cyber operations in and from

[13] Thomas Rid's article, "Cyber War Will not Take Place," is a good example of an otherwise very intriguing argument undermined by an overconcentration on definition as a theoretical foundation. He uses a Clausewitzian definition of war to argue that because cyber attacks have not in the past met the definitional requirements of violent, instrumental, and political, they do not constitute war but rather forms of sabotage, subterfuge, or espionage. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2011): 6-7, 16-27. While this may be true (and that is debatable), it obscures the more salient aspects of conflict by, with, and through cyberspace. Besides, one might just quote a similarly respected scholar of war, Sun Tzu, whose definition of war is considerably broader and includes victory without engagement, and immediately derail the argument. Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 2005), 62, 115. It is more interesting to contemplate how effects in cyberspace can affect relationships outside of it, regardless of how they are characterized. It is less interesting to debate whether or not they constitute "war" as defined by a singular human being, no matter how revered that human being may be in the hallowed halls of military institutions around the world. However they are characterized, effects in cyberspace are important in the context of conflict.

[14] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 24.

[15] Martin C. Libicki, "Military Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 276.

cyberspace."[16] The terms are difficult to pin down. The word "cyberspace" is widely used interchangeably with both the Internet and the World Wide Web, neither of which accurately reflects its nature. The former is a collection of hardware, a network of machines, while the latter is a system of linked documents. Cyberspace is perhaps more accurately conceived of as a metaphor.[17] In the context of governmental actions and international relations, decisions regarding what to include or exclude from cyberspace have "significant implications for the operations of power, as [they] determine the purview of cyberspace strategies and the operations of cyber-power."[18]

For purposes of clarity and simplicity, this analysis will consider cyberspace using David Betz's and Tim Stevens's concept of a "global fluid,"[19] an inclusive model that encompasses all three layers of Martin Libicki's physical-syntactic-semantic model.[20] This inclusive metaphor of a fluid more accurately captures the concept of cyberspace as structured by networks and machines, but affected and acted upon by humans, organizations, and contexts outside of such technological bounds. "A global fluid like cyberspace cannot simply be dismantled like a house or a car, nor can its parameters be easily traced, nor its behaviour readily predicted: cyberspace is in a state of constant flux."[21] This broad definition will allow the analysis to explore the nature of cyberspace and operations through it rather than engage in a prolonged debate regarding who are what is included in any given space. To this end, the use of "cyber" as modifier (e.g., "cyber advocate") is intended to connote a reflection of this broad conception of cyberspace and those who operate within or interact with it.

[16] John B. Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 211.

[17] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London, UK: The International Institute for Strategic Studies, 2011), 13.

[18] Betz and Stevens, *Cyberspace and the State*, 36.

[19] Betz and Stevens, *Cyberspace and the State*, 38.

[20] Libicki's model consists of three layers: the physical layer, the syntactic layer, and the semantic layer, each one building on the previous. Martin C. Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 12-13. Betz and Stevens describe the physical layer as "the 'hard' technological substrate of cyberspace, consisting of machines and networks," the syntactic layer as "the software and protocols that format and structure digital electronic information and which control computer systems and networksb" and the semantic layer as "the information exchanged, stored and otherwise manipulated in computer networks." Betz and Stevens, *Cyberspace and the State*, 37.

[21] Betz and Stevens, *Cyberspace and the State*, 38.

Bounding the Stage

The most significant constraint of this research is its confinement to the realm of the nation-state. The analysis generally excludes consideration of non-state activity, to include terrorism. The intent is to remain focused on actors who are capable of posing existential and complex threats at the state level. It is hoped that this will simplify discussion in order to establish the feasibility of the overall hypothesis. Furthermore, terrorism generally negates the most unique challenge of operations in cyberspace: the potential for anonymity. Generally, one presumes that in the context of the nation-state, non-attribution is preferred due to the inability to tie actions directly back to the state. In the case of terrorism, on the other hand, attribution is required in order to further an organization's agenda and tie idealistic goals to violence. As one author points out, "terrorists usually take responsibility for their actions. That, after all, is the point: Terrorism–including, presumably, cyber-terrorism–is havoc for political reasons. Unless the political motives for a terrorist attack are acknowledged and publicized, the attack has no purpose."[22] Conceivably, an insurgency could resort to cyber-terrorism as a means of undermining the state's ability to provide security for the populace, but the corollary assumption must be that the insurgents could provide the security the government could not. Barring some sort of cyber hostage situation or blackmail, neither of which would fit the definition of insurgency and therefore not pose an existential threat, this scenario appears highly unlikely.

Moreover, even those who loudly trumpet the call of cyber pandemonium generally concur that the threat posed by non-state actors in cyberspace today is, though of concern, less worrying than the threat posed by a nation-state, whose resources far surpass those of even the most robust non-state organization. The threat of cyber terrorism is "largely a red herring" and, in general, "the two words 'cyber' and 'terrorism' should not be used in conjunction because they conjure up images of bin Laden waging cyber war from his cave."[23] One author estimates that the testbed, manpower, maintenance, planning and coordination skills required for a complex attack

[22] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), 7.
[23] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 135.

(attacks with national strategic effects) would drive at least a six to ten year timeline for a terrorist organization to develop.[24] He notes that although it is "difficult to assess with certainty the risks posed by cyber terrorism…there is strong circumstantial evidence pointing to the conclusion that terrorist groups are limited to launching simple cyber attacks," which he characterizes as harassment, far short of the strategic effects associated with complex attacks.[25] Talking about all threats in the same manner simply because they all involve 0s and 1s is "akin to treating the threat posed by a teenager with a bottle rocket, a robber with a revolver, an insurgent with a bomb or a state with a cruise missile as the same simply because they all involve gunpowder."[26] Stated simply, the first, most important consideration for a nation-state is the threat posed by another nation-state. "Long-lasting disruptions," the kind referred to in the doomsday scenarios that would have real and lasting effects in warfare and international relations, "could probably be pulled off only by a nation-state or its surrogates."[27] Until such time as non-state actors and organizations are able to present an existential threat in cyberspace, public discourse is better served first examining the intricacies of conflict between states.

[24] Irving Lachow, "Cyber Terrorism: Menace or Myth?," in *Cyberpower and National Security* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 444.

[25] Lachow, "Cyber Terrorism: Menace or Myth?," 444, 48.

[26] P.W. Singer, "A Defense Policy Vision," *Armed Forces Journal* (June 2011), http://www.armedforcesjournal.com/2011/06/6462790.

[27] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 113.

Chapter 1

The Sky is Falling

Cyberspace's entrance into the lexicon of modern warfighting has left an indelible impression on practitioners and prognosticators alike. Its integration was initially quiet, seeping into the collective consciousness of civil society and those entrusted with its protection. If its incorporation into everyday life was initially discreet, however, its further assimilation over the last two decades has been anything but. Popular media warns the world to shed the shackles of ignorance and gaze into the abyss of chaos and the attendant dangers faced by every man, woman, and child. To many, the specter of cyber war threatens mankind to an extent that rivals anything before witnessed in the history of warfare, a "quantum leap forward in the level of threat." [1]

Like a wolf in sheep's clothing, cyber stalks every facet of the modern warfighter's life, promising advancements and assured victory but instead introducing dependencies and vulnerabilities at every turn. Worse still, the same wolf visits society writ large, threatening not just modern conveniences but indeed life itself. Rather than a reboot of Enlightenment, the introduction of cyber ushers in an age of potential unparalleled destruction, comparable even to the horrors posed by nuclear war. [2] To be sure, this warning smacks of hyperbole; certainly a keyboard could not rival the danger posed by thermonuclear bombs. But what cyber operations may lack in destructive potential, they make up for in ease of access and speed of delivery. Attackers, already possessed of the advantage of initiative, are now "totally independent of time and place, and…in possession of rapidly renewable arsenals of means of attack that potentially produce global harm."[3] Missile speeds are measured in kilometers per hour, but in some cases, cyber weapons travel at the speed of light. Presidents and premiers hold the codes for nuclear holocaust, but cyber operations, and their potential for destruction, are within

[1] Henning Wegener, "Harnessing the Perils in Cyberspace: Who Is in Charge?" (paper presented at the Disarmament Forum, 2007), 46.

[2] Scott James Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27, no. 1 (2009), http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7/.

[3] Wegener, "Harnessing the Perils in Cyberspace: Who Is in Charge?," 46.

reach of nearly every person who touches the internet. No two-person key turn is required to launch a cyber attack, just a keyboard and mouse.

Upon the Precipice of Cyber Armageddon

Richard Clark, former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, proposes a scenario representative of the tenor found in much of the contemporary writing on the subject:

> Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed in New York, Oakland, Washington, and Los Angeles. Freight trains have derailed outside major junctions and marshaling yards on four major railroads. Aircraft are literally falling out of the sky as a result of midair collisions across the country. Pipelines carrying natural gas to the Northeast have exploded, leaving millions in the cold. The financial system has also frozen solid because of terabytes of information at data centers being wiped out. Weather, navigation, and communications satellites are spinning out of their orbits into space. And the U.S. military is a serious of isolated units, struggling to communicate with each other.[4]

This scenario, while admittedly extreme, is not to be dismissed. Though fantastical, the events described are possible. Clarke offers a number of plausible circumstances that could allow for each of the events to transpire, and if they can transpire separately, there is not much to prevent their simultaneous occurrence. No military genius is necessary to imagine that if one is bad, ten at the same time are worse.

Typically, such scenarios underpin efforts to call attention to a perceived ignorance on the part of governmental and institutional leaders and decision-makers. A push began in earnest in the early 1990s to recognize both the power and risk posed by cyberspace. Many touted the emergence of “strategic information warfare,” considered by some to be another form of warfare altogether.[5] In 1996, a report commissioned for the US Joint Chiefs of Staff warned that “the convergence of vulnerable information infrastructures with the traditional critical infrastructures had resulted in a ‘tunnel of

[4] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 67.

[5] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 309.

vulnerability previously unrealized in the history of conflict.'"[6] The same year, over a decade before the first iPhone would be released, one author referred to "[n]ew technological developments and subsequent uses of information [that] have resulted in innovations and weapons the employment of which can have consequences comparable to those of nuclear weapons, without the attendant physical destruction."[7] Another refers to the 1991 Gulf War as the "first information war," and his characterization of the entire decade reflects familiar visions of "digital Pearl Harbors, cyberstrikes against air traffic control systems, and the manipulation of stock markets," all of which have become favorite scenarios frequently referred to in today's discussions of the future of cyber conflict.[8]

The 1990s witnessed an awakening of sorts regarding the realm of cyberspace, especially as it relates to war. Much of the literature of the time suggested that operations in cyberspace could prove to be the dominant, perhaps even decisive, strategy of choice for the coming century.[9] The same sentiment exists today. In 2010, CNN broadcast a live televised simulation of a successful cyber attack on the United States that opened with "a full-screen shot of the words 'WE WERE WARNED,' as if to leave citizens and policymakers alike in no doubt as to the implications of a failure to secure cyberspace."[10] Best-selling author Mark Bowden opined in 2011 that "[a] successful computer attack could compromise nuclear reactors, electrical grids, transportation networks, pipelines – you name it."[11] As recently as 12 March 2013, senior US intelligence officials assessed cyber threats as a bigger risk than even terrorism, something the US has been *at war* against for the last twelve years.[12] A search of *New York Times* articles alone for the first quarter of 2013 returns 55,200 uses of the word "cyber," with headlines ranging from

[6] Quoted in Andrew Rathmell, "Cyber-Terrorism: The Shape of Future Conflict?," *RUSI Journal* 142, no. 5 (1997): 42-43.

[7] Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters* 26, no. 4 (1996): 90.

[8] Rattray, *Strategic Warfare in Cyberspace*, 310.

[9] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004), 5.

[10] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London, UK: The International Institute for Strategic Studies, 2011), 127.

[11] Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011), 49.

[12] Ken Dilanian, "The World; Cyber-Attacks Outrank Al Qaeda as a Threat; Foreign Online Assaults Are Getting Worse, Intelligence Chiefs Say in an Annual Review," *Los Angeles Times* (2013), http://search.proquest.com/docview/1316029347?accountid=4332.

"Cyberattacks Seem Meant to Destroy, Not Just Disrupt" to "U.S. Demands China Crack Down on Cyberattacks."[13] Some warn that entire societies and perhaps even the entire global economy could be decimated by cyber attacks.[14] Though dissenting voices exist, they are exceedingly rare.[15] As the story goes, warfare at the speed of light and ability to trespass in sovereign, if virtual, territory represents uncharted territory, a no-man's land where laws of physics do not exist and laws of warfare, therefore, may not apply. In the common telling, war's final frontier is artificial, and the ability to operate nearly at will, at least for those with the technology, money, and know-how, represents a continuous, rapidly growing risk of unimagined proportion. While each call to arms is unique, there are some threads common to each of them.

What Will Happen?

A number of theories exist, but most revolve around a central theme. They overwhelmingly predict action directly against civilian populations. Indeed, many theories predict not a gradual targeting of civilians but an almost immediate and primary aim at noncombatants. Joel Brenner, a former inspector general at the National Security Agency and one-time head of counterintelligence for the Director of National Intelligence, warns that "malware has interfered with freight and passenger rail signaling systems, and the government's own reports have concluded that our air traffic control system is vulnerable to attack."[16] In Clarke's scenario, cited earlier, the adversary's first acts include attacks against civilian airliners and trains, as well as operations designed to release poison gas clouds over major metropolitan areas.[17] These sorts of examples are common among predictions about the future of cyber warfare. Though forecasts vary regarding priorities and timelines, they generally warn of attacks on critical

[13] The New York Times, "Search Results," http://query.nytimes.com/search/sitesearch/#/*/from20130101to20130331/ (accessed 27 April 2013).

[14] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 313-14.

[15] In 2001, David Lonsdale posited the existence of a few such dissenting voices, but tellingly referenced only one, Lawrence Freedman, in his citation. In *Cyberspace and the State*: *Toward a Strategy for Cyber-Power*, David J. Betz and Tim Stevens have attempted to stem the tide of cyber hysteria, but their voices caution are by far the exception rather than the norm. Lonsdale, *The Nature of War in the Information Age*, 11, 17.

[16] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 110.

[17] Clarke and Knake, *Cyber War: The Next Threat to National Security*, 65.

infrastructures, normally focused specifically on telecommunications networks, energy infrastructure, transportation infrastructure, and the financial system. "[C]yber-prefixed threats…splashed across the covers of popular books and newspapers….threaten electronic commerce…and the property and well-being of citizens."[18] Further, these forecasts generally portray an adversary with very little interest in discriminating between civilian and military targets. On the contrary, an undercurrent of expectation runs through most that implies that not only is there little concern regarding discrimination, but that civilians may hold the primary position in the adversary's targeting priorities and that the effects will be immediate, they will be overt, and they will be devastating.

One author opines that the fixation on critical infrastructure is a direct legacy from the sort of strategic bombing that has been attempted since the early days of air power, but especially during Second World War, when air planners sought to destroy Germany's ball bearing industry with the thought that it would break the back of the enemy's war machine.[19] As the world has become more digital, strategic targets have become more accessible; strategic effects have become more achievable. The same author argues that modern conflict will increasingly target the human dimension and as such, the focus will shift from physical things to "what people value and what sustains them within a societal context."[20] Given the increasing reliance on computerization and interconnectivity, a critical and exceedingly vulnerable sector of critical infrastructure is a nation's telecommunications and information network.

In many predictions, telecommunications networks themselves are the first and most obvious target.[21] These would be considered attacks *against* computers or networks. Logically, they present the most accessible objective with the greatest potential payoff. If a system relies on the exchange of information, rather than affecting the information, why not destroy the means to transmit it? Additionally, modern

[18] Betz and Stevens, *Cyberspace and the State*, 11.
[19] Douglas H. Dearth, "Critical Infrastructures and the Human Target in Information Operations," in *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, ed. Alan D. Campen and Douglas H. Dearth (Fairfax, VA: AFCEA International Press, 2000), 203.
[20] Dearth, "Cyberwar 3.0," 203.
[21] Richard Clarke's *Cyber War* contains a good example of this common theme. In his hypothetical scenario, collapse of the military's data networks are the first sign that the nation is undergoing an attack. Clarke and Knake, *Cyber War: The Next Threat to National Security*, 64-65. See also J. Brenner, *America the Vulnerable*, 118.

societies rely increasingly on digitization and connectivity to increase productivity and efficiency in other sectors. Power grids are computerized. Aspects of air, sea, road, and rail commerce are increasingly automated and centrally managed. Nations' financial sectors have gone global. From a strategic point of view, telecommunications networks seem to represent a perfect target, the ball bearings of the digital age.

Additionally, telecommunications networks have the added benefit of higher vulnerability. By definition, they are accessible via cyberspace. Certainly, as dependence on telecommunications networks has increased, so have capabilities and efforts to digitally secure them. Most sensitive infrastructure networks are logically and physically separated from the wilds of the internet, for instance. Any connectivity, though, even among computers on a theoretically isolated network, necessarily introduces vulnerability. The more open the networks must be to facilitate exchange of information, the more vulnerable they become to sabotage. Telecommunications networks may also tend to be physically vulnerable. Central telephone exchanges, trunk distribution facilities, and wireless nodes abound in major metropolises, often devoid of nearly any security and, according to at least one author, far short of anything remotely approaching a level commensurate with their value.[22] Although many countries are beginning to address these concerns, the sheer numbers and proliferation of vulnerabilities suggests that they will exist for the foreseeable future.

In addition to the telecommunications infrastructure itself, several other key sectors such as energy, transportation, and financial are frequently mentioned as likely targets of cyber attacks.[23] As opposed to attacks on the telecommunications systems themselves, these attacks, which use cyberspace as a means of *access*, could be considered attacks *by* or *through* cyberspace. Their targets are not necessarily the

[22] Alan D. Campen and Douglas H. Dearth, *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (Fairfax, VA: AFCEA International Press, 2000), 205.

[23] The 2010 US National Security Strategy warns of the vulnerability of power grids as well as transportation nodes and the economic sector. The President of the United States, *National Security Strategy*, 2010, 18, 27, 31. Betz and Stevens note that modern networked societies are becoming increasingly anxious about actors in cyberspace, specifically those that threaten critical national infrastructures. Betz and Stevens, *Cyberspace and the State*, 11. See also Lonsdale, *The Nature of War in the Information Age*, 11. See also Clarke and Knake, *Cyber War: The Next Threat to National Security*, 64-68. See also J. Brenner, *America the Vulnerable*, 141-47. See also David E. Sanger, "In Cyberspace, New Cold War," *The New York Times* (2013), http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all.

computers or networks themselves, but the systems they are attached to and those that they control. Perhaps the most potentially devastating risk, and for that reason most often warned about, is that posed by an attack on a country's energy infrastructure. Senior US intelligence officials warn that the Chinese and Russians have already penetrated the nation's power grid and that Iran has shown interest as well.[24] At the most extreme end of the spectrum lies the threat posed by attack on a nuclear reactor. If an enemy could gain access to the sophisticated controls of a nuclear power station, it could conceivably cause a meltdown or, worse, an explosion.[25] Barring an attack on a nuclear plant directly, the grid itself could be attacked: safety measures could be overridden so that transformers could be overloaded and destroyed and generators made to spin out of control until they self-destructed.[26] The warnings are dire. "Sophisticated attacks using advanced, persistent malware are increasing, and…the risk of large-scale disruption to the grid and other critical infrastructure is on the rise. The cost of ignoring this risk could be disastrously high for the nation and could put many firms out of business. Rational businesses and rational government buy down risk, but those who run our critical infrastructure are not doing that."[27] Even regionally such an attack, especially if its effects were sustained, could affect a wider swath of the nation's economy. Those regions not directly affected would still feel an impact as the country raced to discover the cause and worried whether they were next. Susan Brenner, an expert in the field of cyber law, refers to this as an example of "a weapon of mass disruption."[28] In so-called information societies, the entire society is at risk of shutdown in the wake of an attack.[29] Similar to strategies employed during World War II, these sorts of attacks would serve a dual purpose of inhibiting a country's ability to function and, theoretically at least, target

[24] J. Brenner, *America the Vulnerable*, 106. See also Sanger, "In Cyberspace, New Cold War." See also Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S. ," *The New York Times* (2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

[25] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), 45.

[26] Brian Palmer, "How Dangerous Is a Cyberattack?," *Slate.com* (2012), http://www.slate.com/articles/news_and_politics/explainer/2012/04/how_dangerous_is_a_cyberattack_.html. See also Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN.com* (2007), http://www.cnn.com/2007/US/09/26/power.at.risk/.

[27] J. Brenner, *America the Vulnerable*, 115.

[28] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 48-49.

[29] Lonsdale, *The Nature of War in the Information Age*, 11.

the morale of the civilian populace.[30] This same strategy underpins suggestions that warfare in cyberspace will most likely involve attacks on transportation networks.

As the Allies discovered in World War II, the destruction or disruption of transportation networks offers a significant opportunity to cripple a modern nation's industry and economy. Experts estimate that over 5 percent of the US Gross Domestic Product derives from civil aviation, one of the most technologically dependent industries in the world.[31] From satellite-aided navigation and communication to computerized and networked air traffic control, computers are chiefly responsible for keeping planes in the air. Similarly, ships traversing the world's oceans rely on computerized navigation aids, digital communications links, and a host of other systems to deliver almost 90 percent of world trade from one place to another.[32] As with air links, these sea links rely on computerized scheduling and control. The systems that determine what to ship, when to ship it, and where to ship it are all computerized. On land, the story is the same. Railways account for over 40 percent of intercity freight transportation in the United States, to include 70 percent of coal delivered to power plants.[33] As with air and sea, rail transportation is reliant on computerized scheduling, remote sensing to detect problems, and a host of other technology-enabled capabilities to enable centralized management as well as streamlined operations. Additionally, though road systems are generally not thought of as very technologically advanced, the cars and trucks that traverse them are, and affecting those could threaten the integrity of the system as well. Again, scheduling and distribution processes of major shipping companies are heavily reliant on computer systems. Furthermore, though initially merely an inconvenience, long-term and widespread interruption of signaling systems could develop into major impacts. Simply put, the transportation sector is a country's circulatory system. Its degradation would seriously undermine a nation's ability to operate.

[30] It is important to remember here that we are not discussing (yet) whether the strategy will work. There is a strong case to be made against the efficacy of targeting civilian morale. At this point, we are merely examining the logic [behind] these oft-cited target sets.

[31] Federal Aviation Administration, *The Economic Impact of Civil Aviation on the U.S. Economy* (2011), 5.

[32] United States Environmental Protection Agency, *Transportation Modal Shares of World Trade and U.S. Trade with the World, 2008* (2008).

[33] United States Government Accountability Office, *Freight Railroads: Industry Health Has Improved, but Concerns About Competition and Capacity Should Be Addressed* (2006), 11.

Finally, the system that some argue poses the largest threat to a country's stability is its financial sector. Financial transactions at all levels of the global economy increasingly occur via ones and zeroes, not physical dollars and cents. On a micro level, many people receive banking statements only electronically, with no paper record of the virtual dollars they hold in banks they never visit. Institutionally and internationally, virtually all financial transactions are conducted electronically. A blow to the financial sector has the potential not only to erase personal life savings, it could conceivably bankrupt a company at the touch of a button, were that button able to zero out a company's holdings in a major bank or commodities exchange, for example. Short of financial Armageddon, an enemy could simply slow down or stop financial transactions from happening. The United States witnessed the potential wreckage this could create during the US housing crisis and subsequent freeze of credit from 2007 to 2010. The American economy experienced what some called "The Great Recession" largely as a result of depressed lending.[34] A blow to *all* financial transactions could be devastating. In addition to the direct problems such an attack would impose, there might be a crisis in confidence, leading many to withdraw their money, the impact of which could be even more devastating. A country's economy could be shattered if investment dried up and money moved overseas.

Why Will it Happen?

Having identified "what" might happen, it is now time to turn to the "why." Here too, a number of theories exist as to why this war will be triggered and why it will look the way it will. Given the rather urgent tenor of contemporary warnings regarding the current geopolitical landscape in cyberspace, there must be an underlying force at the root of the momentum toward conflict. Clarke points to the capacity of cyber to bring parity to the battlefield through asymmetric operations.[35] In his view, Chinese doctrine "provides a blueprint for how weaker countries can outmaneuver status quo powers using weapons and tactics that fall outside the military spectrum."[36] Joel Brenner asserts that China "would target the communication and control nodes and so lead us to distrust our

[34] Federal Reserve Bank of San Francisco, "Ask Dr. Econ," http://www.frbsf.org/education/activities/drecon/2012/Dr-Econ-q3.html (accessed 27 April 2013).
[35] Clarke and Knake, *Cyber War: The Next Threat to National Security*, 50.
[36] Clarke and Knake, *Cyber War: The Next Threat to National Security*, 50.

own systems and undermine our decision making, operations, and morale."[37] Unfortunately, neither examines very closely the "why" question.

Clarke correctly points out that no America has ever experienced anything near the kind of damage he describes in his hypothetical attack.[38] He also correctly points out the precise reason why: no nation has ever judged infliction of this kind of devastation and destruction (whether pursued through cyberspace or by other means), and the attendant risk of retaliation, to be within its own best interest.[39] Would that Clarke had spent a bit more time exploring this subject, for it is at the heart of the "why" discussion. What about today's environment has changed that would make this sort of calculus work when it never has in the past? Clarke alludes to a possible change, but only briefly. At the very end of his discussion, he relates an imaginary conversation with the President regarding the challenge of retaliation given the fact that there remains significant confusion regarding the origination of the attack. Here, Clarke obliquely refers to the problem of attribution, almost as if to say that the problem of anonymity were enough to inspire action where it would otherwise be constrained. The question that remains, though, and one that will be addressed in a later chapter, is whether this change is enough to alter the mathematics of national interest.

Some suggest, for instance, that the Chinese may leverage cyber capabilities to bypass and mitigate any disadvantage they might have facing a conventionally superior competitor such as the United States.[40] They argue that the asymmetric advantages available in cyberspace offer would-be adversaries an ability to balance power against a conventionally dominant opponent. According to this logic, whereas a country may be unable to compete with either quality or quantity of weaponry in the conventional realm, cyberspace offers an environment where brains can more easily make up for brawn. The cost of a stealth fighter jet may be prohibitive, but the cost of training a cyber warrior to take the fight to the enemy, especially one as reliant on cyberspace as the United States, might be considered relatively negligible. Two senior colonels from the People's Liberation Army said in 1999 that even the common man would be astonished at how

[37] J. Brenner, *America the Vulnerable*, 135-36.
[38] Clarke and Knake, *Cyber War: The Next Threat to National Security*, 67.
[39] Clarke and Knake, *Cyber War: The Next Threat to National Security*, 68.
[40] J. Brenner, *America the Vulnerable*, 135. See also Clarke and Knake, *Cyber War: The Next Threat to National Security*, 52-53.

"commonplace things that are close to them can also become weapons with which to engage in war."[41] David Kilcullen, a respected counterinsurgent expert, appears to bolster the sentiment, asserting that conventional US military capabilities are today so vastly superior to the rest of the world's that no adversary would be likely to fight using conventional means. He agrees that an antagonist's strategy would likely include some sort of operations in cyberspace and points out that conventional dominance may itself induce others to balance against the United States in cyberspace, where the playing field would be more level.[42]

While these arguments are compelling, they are in reality more about why cyber warfare *might* happen than about why it *will*. The scenarios describe what *could* happen and the theories offer plausible causes. However, given the power of these cyber operations, words like "might" and "could" are insufficient. A significant piece of the discussion is missing.

What is Missing?

A key dimension is missing from many of these stories. Specifically, most fail to discuss the likelihood of these scenarios. They tend to focus on the *what if* instead of the *why*. Clarke himself draws a comparison between cyber and nuclear warfare, but then fails to address the fact that in the nearly 70 years since nuclear weapons first became part of national arsenals, they have been used only once. The problem of attribution in cyber operations is certainly germane to the discussion, but it is a complex issue, deserving of more than the passing reference Clarke offers. The problem of attribution may indeed be a causal factor in predictions of increasing pandemonium in cyberspace, but that conclusion is neither inherent nor self-evident. In fact, the constant discussion and assumed ability of non-attribution to completely change the calculus of war often threatens to overshadow consideration of any possible alternative for cyber warfare's future.

In an effort to rouse interest from the public and governmental policy- and decision-makers, well-meaning cyber advocates and sages may have taken a step too far;

[41] Liang Qiao, Al Santoli, and Xiangsui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America* (Panama City, Panama: Pan American Publishing, 2002), 17.

[42] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford ; New York: Oxford University Press, 2009), 3, 22-23.

the dangers of what *could* happen may have blinded them to the likelihood of whether it *will*. In offering tacit or overt warning that these scenarios may happen, they risk a further, larger inference that they will. Certainly, the government must plan for contingencies, but calls for preparation must not escalate to fear-mongering. To the extent that cyber advocates avoid the hard discussion of probability, they risk doing just that. In an effort to garner attention and shed light on a subject deserving of it, they may have inadvertently set fire to it, conflating risk and vulnerability with likelihood. Many of the claims offered by cyber enthusiasts exceed believability and, as such, threaten to undermine the very message they wish to convey.[43] Much of the rhetoric appears to boil down to a "we can, therefore we will" mentality, but this viewpoint incorrectly correlates capacity with intention, something history warns against. "Vulnerability alone does not lead to strategic success."[44] While cyber warfare may indeed run the risk of devolving into the Armageddon often warned of, there is no reason to believe it is preordained. Man has been here before. Cyber weapons are only the latest to experience the seductive logic of determinism. As the next chapter demonstrates, prominent leaps forward in technology and destructive power have not necessarily led to unrestrained use. In fact, it appears that in at least three cases of particularly destructive and indiscriminate weapons, man has chosen to voluntarily restrict use, puncturing the intuitively logical but fallacious claim that capability implies probability.

[43] Leigh Armistead, *Information Warfare: Separating Hype from Reality* (Washington, DC: Potomac Books, 2007), 1-3.

[44] Lonsdale, *The Nature of War in the Information Age*, 170.

Chapter 2

Sealing Pandora's Box

This chapter examines the rise and subsequent decline in use of three categories of weapons: landmines, chemical and biological weapons, and nuclear weapons. While each is unique, and the reasoning for their limitation varied, the conglomeration of all three exhibits a powerful trend; namely, that the ability to destroy or kill does not necessarily translate into the fullest expression of that capacity. Despite a pedigree dating back over 2,000 years, landmines, which looked in the 1980s to be accelerating toward unrestricted and indiscriminate use the world over, are banned today in 161 countries. After the gaseous horrors of World War I, many assumed that poisonous gasses would become a permanent feature of all future warfare. Their use since that war, however, has been confirmed in only two instances, both of which were widely decried throughout the international community. Though many warned of a nuclear cataclysm that would exterminate all mankind, somehow the world has survived without a single nuclear weapon having been employed in the nearly 70 years since August of 1945. In fact, in each of the three classes of weapons, multilateral agreements have been developed to stigmatize their employment. Even more striking, the world actually witnessed their use and battlefield advantages, and yet still managed to curtail their use in warfare. Contrary to the determinist view that technology drives forward of its own volition, these examples appear to reflect a prominent role for human choice.[1] Not only was the increasingly destructive and indiscriminate use of these weapons not inevitable, even removing the proverbial lid of first use did not prove irreversible; humanity managed to take substantial steps toward resealing the lid. Further integration into warfare's lexicon was, to a large extent, subordinated to a predominant international norm.

Taken collectively, these examples cover the globe. Examination of some states' signing of the nuclear Nonproliferation Treaty (NPT) may be considered disingenuous, as many states have little chance of acquiring them in the first place and therefore have little to lose by agreeing to it. For that reason, however, those same states could conceivably

[1] Merritt Roe Smith and Leo Marx, *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994), 56-57, 59.

be expected to pursue chemical weapons or rely on antipersonnel (AP) mines as forms of asymmetric defense. The histories of the weapons considered here show that the use of a given technology need not of necessity accelerate to apocalyptic levels. Rather, humanity may in fact choose to limit the use of weapons it deems exceedingly indiscriminate. The development of these weapons and their subsequent nonuse offer instructive alternatives to the future predicted by cyber doomsayers. Contrary to their implicit claim that capacity for destruction begets employment of destruction, the histories of AP landmines, chemical weapons, and nuclear weapons illustrate a tendency to limit their use. This chapter demonstrates that as mankind has opened various Pandora's Boxes, it has time and again made a concerted, and often relatively successful, effort to close them again.

Landmines

The concept of obstacles used to inhibit movement on the battlefield has a long and storied past. As early as 330 BC, devices called caltrops were used by the Greeks to blunt the attacks of Persian war elephants.[2] Early caltrops were devices consisting of at least four spikes projecting from a ball in such a way so that three of the spikes form a stable base and the fourth points up as a hazard for animal hooves or tires.[3] By the Middle Ages, anti-mobility devices had made their way to Europe where smiths improved and simplified their design by removing the balls and simply twisting two double-pointed strips of iron together.[4] These devices were still in use extensively as recently as the Vietnam War, where the US Air Force used them to interdict the enemy's primary supply route, the Ho Chi Minh Trail.[5] The concept of anti-mobility is fundamental to battlefield operations. Mere spikes were acceptable, but they could be swept from one's path with relative ease. Warfighters needed something different, something more effective. Enter the landmine.

[2] William C. Schneck, "The Origins of Military Mines: Part I," *Engineer* 28, no. 3 (1998), http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=1123648&site=ehost-live&scope=site&custid=airuniv.

[3] Robert W. Reid, "Diabolical in Its Simplicity, the Ancient, Durable Caltrop," *Military History* 15, no. 3 (1998), http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=841092&site=ehost-live&scope=site&custid=airuniv.

[4] Reid, "Diabolical in Its Simplicity, the Ancient, Durable Caltrop."

[5] Schneck, "The Origins of Military Mines: Part I."

The History of the Landmine

The landmine traces its ancestry to actual mines, or tunnels, first used in the mid-ninth century. During that time period, the Assyrian Army used engineer soldiers to drive tunnels (mines) under or through enemy walls and fortifications in order to "gain access to fortified areas or to create a breach large enough for a full-scale attack."[6] Their method, while crude, was revolutionary at the time. As the Assyrians dug, they braced the tunnel with wooden supports which, upon completion, they would burn, causing it and fortification above it to collapse.[7] At about the same time, on the opposite side of the Asian continent, another groundbreaking development was underway. Though the origin of black powder (ancestor to what is today commonly referred to as "gunpowder") is unclear, academics generally agree it was developed in ninth century China by alchemists searching for an "elixir of immortality."[8] Ironically, they discovered something quite the opposite. Rather than immortality, these ancient Chinese alchemists discovered a substance responsible for the deaths of millions of men for the next 1200 years. The eventually experimented with their newfound capability to create crude landmines, but their use was infrequent.

The first use of explosive landmines in the West was in 1547, when Samuel Zimmermann of Augsburg began to bury one or more pounds of black powder around fortresses. These early devices were actuated by stepping on them or by tripping a wire that activated an igniter. They too were used somewhat infrequently due to their susceptibility to dampness and need for constant maintenance.[9] The moisture problem was overcome in the 1800s with the introduction of explosive shells and percussion caps. The first use of modern landmines is attributed to Captain Gabriel J. Rains of the Confederate States Army.[10] He first experimented with what were then truly improvised explosive devices during the Seminole Wars, developing booby traps in an attempt to

[6] Schneck, "The Origins of Military Mines: Part I."

[7] Schneck, "The Origins of Military Mines: Part I."

[8] Jack Kelly, *Gunpowder: Alchemy, Bombards, and Pyrotechnics: The History of the Explosive That Changed the World* (New York: Basic Books, 2005), 3-4.

[9] Schneck, "The Origins of Military Mines: Part I."

[10] Its origin in the United States is even more compelling in light of the fact that it is one of the only countries not to sign the ban treaty. International Campaign to Ban Landmines, "States Not Party," http://www.icbl.org/index.php/icbl/Universal/MBT/States-Not-Party (accessed 27 April 2013).

protect his outnumbered and constantly ambushed troops.[11] Later, during the American Civil War, Confederate troops emplaced thousands of “land torpedoes” (booby-trapped artillery shells) in and around key cities ranging from Richmond, Virginia, to Savannah, Georgia.[12] From their birth, the morality of landmines was debated vigorously, presaging debates that would gain momentum as their use became more widespread. After then-General Rains directed the placement of the first landmines, his own commanding officer, General James Longstreet, forbade further placement, calling their use neither a “proper [nor] effective method of war.”[13] General Longstreet was eventually overruled by the Confederate Secretary of War, who deemed their use acceptable, provided it was in pursuit of a definite military advantage and not merely used for outright killing.[14] Even some Confederate troops described their use as barbarism, and Union leadership characterized their enemies’ conduct as “most murderous and barbarous.”[15] This debate foreshadowed deliberations that would continue through the present day.

Landmines were employed continuously, if intermittently, throughout the next 80 years leading up to the Second World War, where their use exploded. World War II marked the evolution of the mine “from a singular device that was designed to cause fear or destruction to the individual, to a multifaceted antipersonnel weapon system that stressed a full-fledged concept of area control.”[16] Additionally, landmine technology continuously evolved in an effort to counter improved clearing procedures and techniques, resulting in a downward spiral of reactionary developments that have complicated removal or clearing of minefields and served to increase the danger of landmines exponentially. As militaries began to embrace the technology, their use became more widespread and more deadly. In Korea, a lack of training, combined with the pressure of retreat on the part of United Nations (UN) forces, “sometimes degenerated into pitching them from the back of a moving truck.”[17] Eventually, the signing of an

[11] R. Roy and S. Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," *Department of National Defense Canada* (1999): 4.

[12] Schneck, "The Origins of Military Mines: Part I."

[13] Norman Youngblood, *The Development of Mine Warfare: A Most Murderous and Barbarous Conduct*, War, Technology, and History, (Westport, CT: Praeger Security International, 2006), 42.

[14] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," 5.

[15] Youngblood, *The Development of Mine Warfare*, 42-43.

[16] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," 10.

[17] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," 25.

armistice suspending direct combat laid the foundation for what would become one of the largest minefields in the world, which would become a critical sticking point in efforts to ban the use of mines. The use of air-dropped landmines in Vietnam marked the pinnacle of the problem with long-term tracking and disposal of landmines. Post-combat minefields had always presented a significant problem, as they were rarely cleared and the locations of individual mines were almost never mapped.[18] The introduction of air-delivered cluster-bombs fitted with delayed-action fuses "opened up the possibility of seeding landmines from the air," and the United States took full advantage, significantly hindering any chance of either mapping the weapons' locations or removing them in the future.[19] In the 1980s, the Soviets took a page from the American playbook, deploying from 30 to 50 million landmines across the barren landscape of Afghanistan, a sizable portion of which were airdropped, again with no real hope for mapping or removal.[20] Landmines were by this time widely used; their effectiveness and ease of employment proved irresistible.

Landmines Today: Reducing the Footprint

Today, however, the active use of landmines is almost nonexistent, with a few significant exceptions.[21] Despite what appeared to be a steady rise in their lethality and disregard for the problem of discrimination, the use of landmines started to decrease as the international community began to realize the problems and hazards they presented, especially to civilians. Returning refugees were especially prone to victimization for a number of reasons. Rarely was there any effort to clear landmines post-conflict, nor was there any attempt during conflict to document their locations. Furthermore, in many places (Korea being a prime example), conflict never technically ceased and as such, there was reluctance to completely dismantle defenses. In other countries, the admittedly great danger posed by landmines still pales in comparison to more basic problems like widespread famine and disease. In general, many of the countries most affected by

[18] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," iii.
[19] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," 34.
[20] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," 36.
[21] The notoriety of locations, such as the demilitarized zone on the Korean Peninsula, where the minefield is an active deterrent to cross-border military action, reinforces the importance of, and widespread backing for, the reduction in use of landmines.

landmines have neither the resources nor incentive to remove them.[22] As the international community came to grips with the enduring challenges posed by landmines, people began to search for a way to restrict and ultimately eradicate their use.

According to Jessica Matthews, a Senior Fellow at the Council on Foreign Relations, the collapse of the Soviet Union and subsequent dissolution of the bipolar international system led to a substantial increase in power for non-governmental organizations (NGO) and other non-state actors. As such, a number of issues, heretofore overshadowed by the specter of nuclear Armageddon, began to emerge on the world stage. Matthews suggests that the rise in power of non-state actors increased the role of institutions during that time period, and the result was an invigoration of transnational agreements regarding issues ranging from terrorism to ethnic conflict to drug trafficking.[23, 24] Regardless of the impetus, landmine eradication was pursued throughout the 1990s as a serious issue.[25] In 1997, after six years of multilateral negotiations between advocates of a total ban and those who favored a more limited or no-ban position, an unprecedented breakthrough occurred.[26]

In what the Secretary General of the UN characterized as "a historic victory for the weak and vulnerable of our world," over 120 countries gathered in December 1997 to

[22] Roy and Friesen, "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations," 45.
[23] Jessica T. Matthews, "Power Shift," *Foreign Affairs* 76, no. 1 (1997): 50, 53.
[24] Matthews's liberal institutionalist views regarding the nature of disarmament agreements admittedly comprise only one of many theories regarding the cooperation of states on such agreements. There are likely as many plausible (and multi-faceted) reasons for cooperation as there are countries. Ranging from moral to pragmatic, countries originally signed and have continued to sign for a variety of reasons. Robert Keohane's *After Hegemony,* regarding international regimes, and G. John Ikenberry's thoughts in *After Victory,* regarding international institutions provide significant insight into the incentives states have for signing binding treaties. These are, however, beyond the scope of this research. More to the point, while the motivations that underpin state compliance with international regimes and institutions are interesting and worthy of exploration, this research focuses on the fact that the agreements exist at all. While regimes and institutions exist for a variety of reasons, the details of each are immaterial to the argument at hand. Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 2005). G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars* (Princeton, NJ: Princeton University Press, 2001).
[25] Stuart Casey-Maslen, *Commentaries on Arms Control Treaties*, 2nd ed. (New York: Oxford University Press, 2005), 18-46. See also Eric Moody's in-depth analysis of landmine negotiations throughout the 1990s. E.M. Moody, "Landmines on the Table: A Negotiations Analysis of the Global Campaign to Ban Landmines," (PhD diss., University of Florida, 2008).
[26] Moody, "Landmines on the Table," 13.

sign what would come to be known as the “Ottawa Treaty.”[27] Formally known as the *Convention on the Prohibition of the Use, Stockpiling, Production, and Transfer of Antipersonnel Mines and On Their Destruction*, the treaty dictates that those party to it will never use, develop, produce, transfer, or otherwise acquire landmines; that they will destroy existing stockpiles within four years; and that they will destroy all mines in areas under their jurisdiction or control within 10 years.[28] The negotiations succeeded in gaining the approval of a majority of the countries involved and were hailed as a landmark achievement.[29]

On 3 December 1997, 122 countries agreed to abolish AP landmines. With a few notable exceptions, which are addressed below, a majority of the world’s countries voluntarily submitted to an agreement restricting use of what they viewed as an unacceptable weapon. Today, 161 countries have signed the treaty, a testament to the global appeal of the ban.[30] Skeptics argue that the ban is not as successful as some advocates have claimed, rightly pointing out that of three of the five permanent members of the UN Security Council are among the 35 non-signatories, but that criticism is overly focused on a quantitative measurement and risks missing the larger qualitative aspect of the treaty.[31] Regardless of the relative importance of the countries that did or did not sign the treaty, its establishment and subsequent evolution exemplifies the possibility of a future different from that predicted by determinists. Furthermore, the very fact that

[27] International Campaign to Ban Landmines, *Landmine Monitor Report* (Washington, DC: Human Rights Watch, 1999), 1.

[28] Ottawa Landmines Convention, *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*, 1997.

[29] The convention was negotiated outside the UN in a format similar to the traditional mechanism for negotiation of international humanitarian law agreements that many diplomats considered “anathema” to the more traditional method of consensus-based disarmament negotiations. Casey-Maslen, *Commentaries on Arms Control Treaties*, 27. According to the International Campaign to Ban Landmines, the joint winner of the 1997 Nobel Peace Prize, the process that led to its signing “was unorthodox, historic, and unprecedented…the product of an unusually cohesive and strategic partnership between non-governmental organizations, international organizations, UN agencies and governments. International Campaign to Ban Landmines, "Mine Ban Treaty," http://www.icbl.org/index.php/icbl/Treaty (accessed 21 January 2013).

[30] International Campaign to Ban Landmines, "States Parties," http://www.icbl.org/index.php/icbl/Universal/MBT/States-Parties (accessed 21 January 2013).

[31] Eric Moody’s 2009 doctoral dissertation is an example of such debate over the relative, versus ultimate, success of the treaty. The primary purpose of his study was to ascertain the reasons behind failed negotiations on the part of the United States and other parties, and sought to provide insights that might be valuable to future negotiations. Moody, "Landmines on the Table," 15.

countries' declinations elicit broad condemnation and controversy proves the efficacy of a broad international norm against indiscriminate weapons and warfare.

Far from a simple desire to continue to use indiscriminate weapons, non-signatories have cited a number of reasons for not having signed the treaty. The United States, for instance, requested that a geographical exception be made for South Korea.[32] The argument for exception was predicated on the belief that continued use of the landmines was necessary in order to preserve the armistice on the Korean peninsula, at least until the United States had developed alternatives to the need for landmines.[33] Though the United States acknowledged a desire to reduce the employment of landmines, in areas such as Korea especially, military experts agree that "no other single weapon or tactic can fulfill as successfully the military tasks performed by anti-personnel mines."[34] Pakistan and India's decisions not to ratify the treaty may reflect similar apprehension regarding the border dispute between the two countries. The observer delegation from Vietnam cited similar concerns, stating that while Vietnam welcomed efforts to complete an international comprehensive treaty banning the use of landmines, she could not yet participate in the convention due to territorial defense reasons.[35] Indeed, the need to defend long borders against potential aggressors is the most common justification for the continued use of AP landmines.[36] In the case of the Ottawa Treaty, the nature of the negotiations themselves and the strategies employed by negotiators on both sides were also instrumental in the non-accomplishment of an agreement.[37] Official testimony from several non-signatories indicates that they did indeed have issues concerning landmines and supported some form of ban on them, but all-or-nothing strategies engaged in by various parties at various points in the negotiations was counterproductive to consensus-building.[38]

Still, even those non-signatory states are instructive. Again, they reflect the pressure that the international community can place on a country. That the United States

[32] Casey-Maslen, *Commentaries on Arms Control Treaties*, 40.
[33] Statement by Ambassador Karl F. Inderfurth, Special Representative to the President and Secretary of State for Global Humanitarian Demining (4 December 1997) in Moody, "Landmines on the Table," 248.
[34] Casey-Maslen, *Commentaries on Arms Control Treaties*, 13.
[35] Moody, "Landmines on the Table," 251.
[36] Casey-Maslen, *Commentaries on Arms Control Treaties*, 8.
[37] Moody, "Landmines on the Table," 12, 35-36.
[38] Moody, "Landmines on the Table," 28, 66, 248-49, 51, 62

would struggle as mightily as it did to obtain provisions that would allow it to sign is a testament to the importance and power of the treaty itself. Granted, the pressure has not (yet) coerced the United States into signing the treaty, but the decision expends political capital and diminishes potential diplomatic influence. Additionally, many of those countries who have not signed are nonetheless going to great lengths to comply with significant portions of the spirit of the treaty.

The United States representative to the Ottawa Conference, for instance, noted that President Clinton was the first world leader to call for the elimination of antipersonnel landmines during his speech to the General Assembly in 1994. Furthermore, he noted, the President had made permanent a long-standing moratorium on the transfer and export of landmines and had, as of 1997 destroyed over 1.5 million antipersonnel landmines and was on course to destroy another 1.5 million by the end of 1999.[39] Even prior to the 1997 Ottawa Treaty, the UN General Assembly had already adopted a number of resolutions restricting the usage of antipersonnel mines and directing further efforts to "seek solutions" to problems caused by landmines.[40] In 2011, the United States and Norway were the top two donors in support of mine action, having contributed between them nearly 40 percent of the total funding worldwide.[41] In 2011, the International Campaign to Ban Landmines (ICBL) found evidence of three countries actively using antipersonnel landmines; in 2012 that number fell to only one.[42] Since the Convention went into effect in 1997, the United States has voted in favor of every annual resolution of its support, "an important [indication] of their support for the ban on antipersonnel mines and the objective of its universalization."[43]

The agreement, though far from unanimous, is an important example of the potential for de-escalatory behavior. Contrary to the dystopian view of technology as a privileged and unitary driver of future human endeavor, the Ottawa Treaty illustrates the viability of social constructivist forces. Ultimately, the ratification of the treaty by 161 countries reflects an important lesson: While not without room for improvement, the

[39] Statement by Ambassador Karl F. Inderfurth, Special Representative to the President and Secretary of State for Global Humanitarian Demining (4 Dec 1997) in Moody, "Landmines on the Table," 248.
[40] Casey-Maslen, *Commentaries on Arms Control Treaties*, 30.
[41] International Campaign to Ban Landmines, *Landmine Monitor Report 2012* (2012), 47.
[42] International Campaign to Ban Landmines, *Landmine Monitor Report 2012*, 2.
[43] International Campaign to Ban Landmines, *Landmine Monitor Report 2012*, 12.

Ottawa Treaty reflects a turn *away from* escalation. In 1997, and in the nearly 16 years hence, a large part of the international community has shown a tendency to shun these indiscriminate weapons, which runs counter to the determinist notion of inevitability. Having come to grips with the indiscriminate nature of AP landmines, mankind recoiled and limited their use. Regardless of the international community’s final calculus, the impetus behind the global condemnation of the landmine was the threat it posed to non-combatants. Insofar as the world has acted to eliminate their use, the global community has continued a trend toward the pursuit of increased discrimination.

Chemical and Biological Weapons

Though chemical and biological weapons, due to their often-similar delivery system (gas), are sometimes mistakenly combined, they are two distinct classes of weapons and are treated as such on the international stage.[44] Chemical weapons initially burst onto the world stage, blanketing the battlefields of World War I before suddenly vanishing, nearly as quickly as they had appeared. Modern biological weapons,[45] for their part, have almost never seen the light of day.[46] A single agreement, the Geneva Protocol of 1925, banned the first use of both “asphyxiating, poisonous, or other gases, and of all analogous liquids, materials or devices” (chemical weapons) and “bacteriological methods of warfare” (biological weapons).[47] However, history shows that mankind draws a distinct line between the two categories of weapon. An international ban on the development and testing of biological weapons went into effect in 1975, but chemical weapons would not be the subject of a comparable agreement until two decades later. The histories of chemical and biological weapons are interesting given

[44] This section will examine the history of chemical weapons to a greater extent than biological. Modern biological weapons, as alluded to later in this section, have generally been considered separately from chemical weapons and, as such, have been limited in their scope of employment. Their place on the world stage, while important, is less instructive than that of chemical weapons.

[45] The term “modern biological weapons” as used in this context refers to poisoned weapons; i.e., bombs filled with a biological agent, such as those developed in the robust programs of the Soviet Union and United States following World War II, versus poisons used *as* weapons. Attempts to introduce disease through animal infections or water poisoning were reported in World War I by the Germans and World War II by the Japanese. Outside of the Japanese effort, however, which is thought to have succeeded in spreading epidemics among the Chinese, incidents of widespread contamination have not been reported. Friedrich Frischknecht, "The History of Biological Warfare," *EMBO reports* 4 (2003), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1326439/.

[46] George Bunn, "Gas and Germ Warfare: International Legal History and Present Status," *Proceedings of the National Academy of Sciences* 65, no. 1 (1970): 253.

[47] Bunn, "Gas and Germ Warfare," 255.

that despite the considerable length of time it took to gain substantial international agreement sanctioning their development, employment remained virtually non-existent. Their stories reflect an environment that has chosen to limit the use of non-discriminatory weaponry.

The Very Brief History of Germs in Modern War

Today, 167 nations are party to the Biological Weapons Convention with another 12 having signed but not yet ratified.[48] Those acceding to the treaty agree "never in any circumstances to develop, produce, stockpile or otherwise acquire or retain microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; [or] weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict."[49] Crude forms of biological warfare have been recorded since ancient times. The Greco-Romans first used methods of biological warfare during the Carthaginian Wars in the 5th Century BC, when they poisoned food and water sources with animal carcasses.[50] The Black Death is thought to have been introduced to the Crimean city of Caffa via biological warfare. According to accounts at the time, the Mongols flung carcasses infected by the plague over its walls during their siege of the city in 1346.[51] The British were rumored to have attempted to pass infected blankets to the Native Americans during Pontiac's Rebellion.[52] The only recorded use of widespread biological warfare in the twentieth century was the use of well-poisoning tactics and the introduction of infected fleas used by Japan against China in World War II.[53] Though the causal relationship of biological weapons treaties and non-use is debatable, both appear to at least reflect a near-universal abhorrence of the potential effects of biological weapons.

[48] The United Nations Office at Geneva, "Membership of the Biological Weapons Convention," http://www.unog.ch/80256EE600585943/(httpPages)/7BE6CBBEA0477B52C12571860035FD5C?OpenDocument (accessed 22 January 2013).

[49] The United Nations Office at Geneva, *The Biological Weapons Convention*, 1972, 2.

[50] Emil Lesho, David Dorsey, and David Bunner, "Feces, Dead Horses, and Fleas: Evolution of the Hostile Use of Biological Agents," *Western Journal of Medicine* 168, no. 6 (1998), http://search.proquest.com/docview/200466980?accountid=4332.

[51] Mark Wheelis, "Biological Warfare at the 1346 Siege of Caffa," *Emerging Infectious Diseases* 8, no. 9 (2002), http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=7433556&site=ehost-live&scope=site&custid=airuniv.

[52] Carl Waldman, *Atlas of the North American Indian*, 3rd ed. (New York: Facts on File, 2009), 141.

[53] Frischknecht, "The History of Biological Warfare."

Chemical weapons, on the other hand, have made a number of appearances on the world stage. Like landmines, however, they appear to have been, to a great extent, put back in the proverbial box. They have not been completely eradicated worldwide and their use is occasionally rumored. Nonetheless, the existence of almost unanimously agreed upon ban and immediate condemnation associated with their use underscore the strength exerted by the international community in an attempt to reverse the trend and eliminate them from the globe.

Worse Living Through Chemistry: Pre-World War I

The first recorded use of poisonous gas in war is credited to the Spartans during the Peloponnesian Wars. In an effort to choke the defenders of the cities of Platea and Belium, the Spartans soaked wood with pitch and sulfur and burned it under the walls of the two cities.[54] More recently, in 1855, during the Crimean War, British Admiral Lord Dunadold devised a plan to use sulfur gas against the Russians.[55] The plan was included in *The Panmure Papers*, "An extremely dull record of an extremely dull person, only rended interesting by the one portion, concerned with the use of poison gases, which, it is said, 'should never have been published at all.'"[56] When the plan was originally submitted, the British declined to adopt it. Though they judged the scheme feasible, they considered the effects "so horrible that no honorable combatant could use the means required to produce them."[57] This reticence reflects a concern regarding the use of chemical weapons similar to that found in debates concerning the use of antipersonnel landmines. For reasons of morality, chivalry, culture, or otherwise, the use of a weapon with so little hope of discrimination was avoided. In fact, as the following discussion illuminates, even before the first recorded use of lethal gas in World War I, the international community recognized the danger of chemical warfare and sought to stop it before it began.

At least as early as 1899, with the establishment of the first Hague Convention, mankind attempted to curtail the use of chemicals in warfare. Admittedly few in number, the 27 countries signing the agreement nonetheless signaled a belief in the prospect of an

[54] Clarence J. West, "The History of Poison Gases," *Science* 49, no. 1270 (1919): 413.
[55] Crimean Texts, "The Panmure Papers, Volume 1," http://crimeantexts.russianwar.co.uk/sources/panmure/pcont08.html (accessed 22 January 2013).
[56] West, "The History of Poison Gases," 413.
[57] West, "The History of Poison Gases," 414.

international regime that could restrict the use of chemicals.[58] The 1899 agreement was focused on banning certain types of technology in war. In the case of chemicals, it expressly forbade the "use of projectiles the object of which is the diffusion of asphyxiating or deleterious gases."[59] Eight years later, the 1907 Hague Convention reinforced the sentiment, prohibiting any employment of poisons or poisonous weapons.[60] Though two technologies forbidden by the Conventions, bombing from the air and chemical weapons, were used less than two decades later, the agreements were important milestones in the restriction of chemical weapons. Together, they formed a foundation that withstood the setbacks of World War I and set the stage for a broader agreement in 1925.[61]

Blanketing the Battlefield: Chemicals in World War I

In April 1915, the Germans unleashed over 150 tons of Chlorine gas against the French in Ypres, Belgium, marking the first time in modern history that a country had employed a lethal chemical attack in war.[62] Although they had begun research into the possibility of chemicals on the battlefield, the Allies had yet to employ any lethal chemicals on the battlefield prior to the German attack of 1915.[63] The French had likely used a form of tear gas prior to the Germans' use of Chlorine, but they contended it was not an "asphyxiating or deleterious" gas as prohibited by the Hague Conventions, and was therefore permitted under the language of the Hague Conventions.[64] After the Germans opened the technological door, the Allies felt that they had no choice but to step

[58] Of the 28 participants, all but the United States signed on to the agreement. The American representative, Captain Alfred Thayer Mahan, cited the as yet impracticality of canister-delivered gas as the primary reason for refusing to sign. Bunn, "Gas and Germ Warfare," 253.

[59] Yale Law School, "Laws of War: Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases; July 29, 1899," http://avalon.law.yale.edu/19th_century/dec99-02.asp (accessed 22 January 2013).

[60] West, "The History of Poison Gases," 415.

[61] Richard Price, "A Genealogy of the Chemical Weapons Taboo," *International Organization* 49, no. 1 (1995): 92.

[62] There is speculation that the German use of gas in World War I was inspired by Dunadold's plan. While *causal* linkage is unlikely (the Germans would have resorted to chemical warfare with or without the speculated link to the Panmure Papers), there does appear to be evidence that the Germans somehow got hold of his plan and used it as a foundation to build their own chemical weapons program. Charles Stephenson, *The Admiral's Secret Weapon: Lord Dundonald and the Origins of Chemical Warfare* (Rochester, NY: Boydell, 2006), 141-43. See also West, "The History of Poison Gases," 414.

[63] Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz, *Medical Aspects of Chemical and Biological Warfare*, Textbook of Military Medicine Part I, Warfare, Weaponry, and the Casualty (Washington, DC: Borden Institute, 1997), 13-14.

[64] Bunn, "Gas and Germ Warfare," 253.

through.[65] When the armistice was signed in 1918, approximately one million of the 26 million casualties suffered on all sides were caused by gas. For the United States specifically, who did not enter the war until 1917, two years after the first lethal use of gas, the ratio was 72,000 gas casualties out of a total of 272,000 or about one fourth.[66] For the men in the trenches, the threat of gas hung heavy throughout the war.

In modern times, the use of chemical weapons appears to have carried with it a tacit acknowledgement of the associated moral dilemma of using such an indiscriminate weapon, and World War I was no different. Use of chemicals during The Great War invariably stirred debate even as their necessity (and centrality to future warfare) was professed. Writing in 1919, only months after the close of World War I, Dr. Clarence West[67] declared that "[w]hile there was certain hesitation on the part of the Allies about adopting gas warfare, it was not long before they were forced to do so, because of its continued use by the Germans."[68] Despite these professed misgivings, Dr. West went on to credit "Gas Warfare" with enabling the Allies to win the war and declared its use "one of the deciding factors in every large battle."[69] On the opposite side of the war, the Germans expressed similar objections. General von Deimling, commanding general of the German 15th Corps in front of Ypres, said as much himself: "I must confess that the commission for poisoning the enemy, just as one poisons rats, struck me as it must any straight-forward soldier: it was repulsive to me."[70] General von Deimling's views express a common sentiment, often overlooked among warfighters throughout history. Generally, they view themselves as professionals, engaged as they are in the *profession* of arms. Despite a requirement to kill, they tend to prefer to think of themselves as more

[65] Amos A. Fries and Clarence J. West, *Chemical Warfare* (New York: McGraw-Hill Book Company, inc., 1921), http://books.google.com/books/reader?id=kGGpuj9s-tIC&printsec=frontcover&output=reader&pg=GBS.PR2, 14.

[66] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 24.

[67] Dr. West was a member of the Information Department at Arthur D. Little, Inc., a consulting firm. Today, the company bills itself as "the world's first consultancy," having "been at the forefront of innovation for more than 125 years." Arthur D. Little, "About Us," http://www.adlittle.com/about-us.html (accessed 23 January 2013).

[68] Clarence J. West, *Chemical Warfare* (Cambridge, MA: Arthur D. Little, inc., 1919), http://books.google.com/books/reader?id=G3AwAQAAMAAJ&printsec=frontcover&output=reader&pg=GBS.PP1, 1.

[69] West, *Chemical Warfare*, 1.

[70]Frederic Joseph Brown, *Chemical Warfare: A Study in Restraints* (New Brunswick, NJ: Transaction Publishers, 2006), 41.

than butchers. By all means, they must win, but if possible, they would prefer it not be at all costs.

The end of World War I brought with it two significant and parallel views regarding chemical warfare. On one hand, those charged with preparing for future wars viewed the use of chemical weapons as inevitable. Two years after publication of his first book, Dr. West teamed with Brigadier General Amos Fries, Chief of the US Army's Chemical Warfare Service (the existence which, in and of itself, is testament to how accepted and expected chemicals were at the time), to write a book detailing the history of chemical warfare in part "because of the future needs of a textbook covering the fundamental facts of the Service."[71] West and Fries considered chemical warfare a fundamental part of future warfare, declaring, "There is no question but that it must be recognized as a permanent and very vital branch of the Army of every country."[72] General Fries's predecessor, Major General William Sibert, wrote in the foreword to the book that "[h]istory proves that an effective implement of war has never been discarded until it becomes obsolete;" and, in reference to the danger posed to civilians by gas clouds, warned that "the population in the area behind the front lines must, if they remain in such range, take their chance."[73] The generals' opinions notwithstanding, some advocated an alternative to this strictly determinist outlook. This second view saw the future of chemical warfare as anything but inevitable. On the contrary, those who possessed this view saw the results of chemical weapons as so abhorrent that the weapons must be eradicated at any cost. This set the stage for the Geneva Protocol of 1925.

The Allied view of German culpability in the matter of chemical warfare during World War I is reflected in the Treaty of Versailles, the agreement that ended the war. The treaty expressly prohibited German use, manufacture, or importation of "asphyxiating, poisonous or other gases."[74] Seven years later, the Geneva Protocol used the same language, complete with the "or other gases."[75] This created an unfortunate ambiguity that plagued chemical weapons disarmament negotiations for the next five

[71] Fries and West, *Chemical Warfare*, vii.
[72] Fries and West, *Chemical Warfare*, vii.
[73] Fries and West, *Chemical Warfare*, ix.
[74] *Peace Treaty of Versailles*, 1919, 87.
[75] The Geneva Protocol, *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, 1925.

decades, with debate over the legality of incapacitating agents (i.e., tear gas) and defoliating agents still raging as recently as the Vietnam War.[76] At issue was the intent of the word “other.” If “other” signified “all other,” then the use of tear gas or defoliating agent was prohibited. If, on the other hand, “other” meant “others similar to the lethal agents used during World War I,” then these chemicals could be used.[77] The debate over semantics aside, one thing was clear: The use of *lethal* gas in warfare had the potential to devastate civilian populations as no other weapon ever had. In Geneva in 1925, the world would take the next step to curb its use.

Dissipation: Constraining Chemicals from 1920 to 1970.

Having witnessed the terrible destruction wrought by chemical weapons during World War I, the international community set out to strengthen agreements barring their future use. In 1925, 38 countries signed the Geneva Protocol. The agreement states that “the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices, has been justly condemned by the general opinion of the civilized world.”[78] The United States initially failed to ratify the Protocol out of disagreement over the use of incapacitants. Though consensus over their use was finally reached in principle in the early 1930s, no treaty to this effect was ever established. Soon, Germany withdrew from the talks and the drumbeat of war grew from a faint whisper to a deafening roar.

Though the 1930s saw the sporadic use of chemicals by the Italians and reportedly by the Japanese, their use was universally condemned.[79] Many credit the 1925 protocol with reversing what was by several accounts an unstoppable trend toward eternal use of chemicals in war. It constrained civilian and military leadership and established the norm of conduct deterring the use of poison gas in war.[80] Indeed, in World War II there was no use of gas on either side, nor was there in Korea. Granted, a mutual fear of retaliation and general lack of preparedness on the part of the combatants vis-à-vis chemical warfare were additional contributing factors, implicitly relegating the moral

[76] Bunn, "Gas and Germ Warfare," 256-58.
[77] Bunn, "Gas and Germ Warfare," 254.
[78] The Geneva Protocol, *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*.
[79] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 34-36.
[80] Bunn, "Gas and Germ Warfare," 255-56.

abhorrence of such weapons to merely one of several factors.[81] Admittedly, it was not "utterly unthinkable for any belligerent to countenance chemical warfare."[82] However, the existence of what one author terms the "peculiar operation of the [chemical weapon] taboo" singularly "raised the threshold of circumstances under which one could justify a resort to" their use, short of complete desperation.[83] Moreover, a significant contributing factor to unpreparedness was the stigma of chemical weapons itself. Fighting for resources and time for chemical warfare preparedness was hindered by the normative and legal challenges to such preparation as well as a general hope that they would not be used.[84] Simply put, it is incredible that even in the face of multiple existential crises, between 1939 and 1953, no belligerent ever resorted to the use of chemical weapons. Though a number of factors were at play, "this nonevent cannot be understood without an appreciation of the necessary role played by the taboo attached to the use of [chemical weapons]."[85] Not until Vietnam, in fact, would the world witness widespread use of airborne chemicals in time of war, this time initiated by the United States.

During the Vietnam War, the United States used both incapacitants (tear gas) and defoliants.[86] The humanitarian justification used by the United States at the time was widely questioned, and as the passage of time has shed light on the actual employment, their use becomes even more questionable.[87] Debate over intent aside, what is more germane to the context of this study was the rationale behind their use. Specifically, whatever the public or private motivations may have been underlying the use of chemicals in Vietnam, the United States never justified their use on the grounds that it

[81] Stockholm International Peace Research Institute, *The Problem of Chemical and Biological Warfare: A Study of the Historical, Technical, Military, Legal and Political Aspects of CBW, and Possible Disarmament Measures*, vol. 4 (New York: Humanities Press, 1971), 21.
[82] Price, "A Genealogy of the Chemical Weapons Taboo," 76.
[83] Price, "A Genealogy of the Chemical Weapons Taboo," 77.
[84] Price, "A Genealogy of the Chemical Weapons Taboo," 75-76.
[85] Price, "A Genealogy of the Chemical Weapons Taboo," 77.
[86] Bunn, "Gas and Germ Warfare," 256-57.
[87] The United States initially proclaimed that the use of tear gas was humanitarian on the grounds it would reduce the number of non-combatants killed and would be used in a way more analogous to riot control than military operations. However, some argue that regardless of the intended or stated justification, the upshot was that the use of tear gas was ultimately often used to flush people out, combatant or civilian, from underground in order to make follow-up kinetic strikes more effective. Similarly, though the United States cast the use of defoliants in a humanitarian light, pointing to the similarity between the chemicals used in Vietnam and those used to control weeds in the United States, there is debate as to whether or not their use did not gradually become aimed at destroying food production in Viet Cong-controlled areas. Bunn, "Gas and Germ Warfare," 256-57.

was not party to the Geneva Protocol. Indeed, throughout the 1960s, the US State Department reaffirmed a strong commitment to the precepts of the agreement, and the United States even went so far as to sponsor and vote for a UN resolution calling for strict observance of the Protocol's principles. The United States continued to support the objective of the Protocol and maintained throughout that its use of incapacitating agents and defoliants was simply not prohibited by its terms. Having interpreted the Protocol as containing no provision against the use of tear gas or defoliants, the State Department took the view that the United States was bound by the Protocol even in the absence of its ratification by the Senate. This interpretation mirrored the case of the Nuremburg trials, in which Germany was convicted of war crimes despite having not been a signatory to the subject treaty. Treaty standards were deemed applicable "simply because these standards had become widely accepted by a great many countries over a long period of time."[88] It again reflects a common trend in human history. Irrespective of treaty ratification and despite the anarchic nature of the international system (or perhaps because of it?), mankind takes a dim view of indiscriminate killing, even in the midst of the horrors of war. General Sibert's assertion notwithstanding, the box can be closed again.

Regardless of one's opinion regarding the veracity of the United States's position vis-à-vis the use of chemicals in Vietnam, the lesson is extremely important: even a world superpower felt considerable pressure to conform to the norms of an international agreement on the use of chemicals in war. Though it did not prevent their use altogether, the United States went to great lengths to justify their use in the world's eyes and spent political capital in order to do so.[89] Far from a foregone conclusion, use of chemicals in war appeared to have gained enough of a negative reputation to limit their use.

Outside of Vietnam, the use of chemical weapons from 1950 to 1970 was extraordinarily rare, especially in light of the dire predictions of the early part of the century. There were reports of their use in the Yemen Civil War, but the evidence was questionable.[90] Many consider the Arab–Israeli Six-Day War of 1967 as the closest the

[88] Bunn, "Gas and Germ Warfare," 257.
[89] Bunn, "Gas and Germ Warfare," 256-58.
[90] Kim Coleman, *A History of Chemical Warfare* (New York: Palgrave Macmillan, 2005), 101.

world has ever come to the open use of nerve agents by both sides in a major war; but ultimately, none were employed.[91]

Between World War I and 1970, the world experienced a period of relative stability regarding chemical weapons. It would not be punctured until the United States's reestablishment of debate over use of incapacitants and defoliants in Vietnam in the 1970s. In the 1980s, the world condemned Sadaam Hussein's use of chemical weapons against Iran, indicating that a norm had indeed been established.[92] The evil may poke its head out of the box from time to time, but the international community had shown that in the case of these horrible and particularly indiscriminant weapons, it will not stand for it. This period, and the world's reaction to the reintroduction of chemicals on the battlefield, will be further examined in the next section.

Chemical Reactions: Gas on the battlefield from 1970 to Today

The decades following 1970 featured an increased focus on chemical warfare. In 1974, the United States Senate finally ratified the Geneva Protocol, still five years after President Nixon had called for it.[93] Evidence from Soviet-made equipment captured during the Yom Kippur War appeared, however, to signal a robust Soviet capability to wage chemical war.[94] The future of chemical weapons seemed poised once again to go in either direction, toward further limitation or, in a reversal of its current course, toward expansion. On one hand, the United States finally agreed to the terms of the Protocol. On the other, some considered the Soviet capability a tacit acknowledgement of the intent to use chemical weapons in future warfare, despite Russian agreement to the Protocol in 1928.[95] In the 1980s, purported use of chemical weapons by the Soviets in Afghanistan further escalated tension and appeared to signal a possible return of chemical warfare to the world stage; but the allegations have never been substantiated.[96] The 1980s did witness substantiated use of chemical weapons elsewhere, however.

[91] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 56-57.
[92] Coleman, *A History of Chemical Warfare*, 109.
[93] Coleman, *A History of Chemical Warfare*, 104-05.
[94] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 65.
[95] Interestingly, it appears no-one considered whether the extensive sophistication of Soviet chemical defense materiel was in fact simply a reasonable reaction to the fact that their principal adversary had not agreed to the Protocol. Robert Jervis's work regarding perception and misperception appears highly applicable in this situation. See Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).
[96] Price, "A Genealogy of the Chemical Weapons Taboo," 78.

In September 1980, Iraq launched an invasion against Iran. In November of that year, reports surfaced that they had begun using chemical weapons against their neighbors, to include mustard gas and the nerve agent Tabun.[97] As the world watched, many predicted a new dawn for chemical warfare. Indeed, one analyst at the time declared that the taboo against chemical weapons had been broken, "thus making it easier for future combatants to find justification for chemical warfare," and he warned that "this aspect of the Iran-Iraq War should cause Western military planners the gravest concern."[98] Then, in 1990, Iraq invaded Kuwait and fears of chemical warfare reached a new high.[99]

When Iraq did not respond to international pressure to withdraw from Kuwait, the United States deployed troops to the region to begin building up a strength capable of forcible removal. Tensions were high and the expectation of chemical warfare was almost universal. Not only had Iraq just used chemical weapons, it publicly announced their intention to use them again if threatened by the United States.[100] Certainly, Iraq possessed the necessary capability and had demonstrated the necessary will. In the event, however, the weapons remained dormant.[101] Again, myriad reasons exist regarding Iraq's non-use. Leading up to the war, some allies expected the war to be chemical "probably from the first hour."[102] The fact that it was not is not easily attributable to a single cause. Plausible theories abound, ranging from a fear of massive (perhaps nuclear)

[97] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 69.
[98] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 69.
[99] To make matters worse, reports had surfaced by this time that Hussein had used chemical weapons on his own people. Within weeks of the close of the Iran-Iraq War, he was accused of using chemical weapons to quash a rebellion by the Kurds, a minority group in northern Iraq seeking independence. Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 69. There were also rumors of his having used chemical weapons to put down a Shi'a uprising in southern Iraq in 1991, but evidence in inconclusive. The Central Intelligence Agency asserts the accusations are true, but the UN conducted an investigation in 1994 and found no evidence of chemical weapons having been used. Central Intelligence Agency, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD*, 2004. Minorities at Risk Project, "Chronology for Shi'is in Iraq," http://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=country&category=&publisher=MARP&type=&coi=IRQ&rid=&docid=469f38a61e&skip=0 (accessed 28 April 2013).
[100] Sidell, Takafuji, and Franz, *Medical Aspects of Chemical and Biological Warfare*, 73.
[101] There remains an undercurrent of skepticism regarding whether or not there may have been sporadic exposure, most of which stems from an attempt to explain the occurrence of so-called Gulf War Syndrome in some veterans returning from the theater. The US Department of Defense and British Ministry of Defense, however, deny any persuasive evidence has been found to substantiate the claims. Jonathan B Tucker, "Evidence Iraq Used Chemical Weapons During the 1991 Persian Gulf War," *The Nonproliferation Review* 4, no. 3 (1997): 114-15. See also Coleman, *A History of Chemical Warfare*, 117-18.
[102] Price, "A Genealogy of the Chemical Weapons Taboo," 77.

reprisal to an attempt to restore some international credibility following the fallout from use of chemicals in the war against Iran. Likely, a combination of many factors played a role in Iraq's decision not to use chemical weapons.[103] No matter what the reason, the fact remains that possession and capability did not beget use. In fact, rather than a downward spiral of ever-increasing chemical battlefields, the 1990s instead bore witness to a seminal event, the creation of the Chemical Weapons Convention. The lid was sealed even more tightly.

In January 1993, after nearly a quarter century of negotiations, the Conference on Disarmament, a multilateral arms control organization tracing its lineage to the beginning of the Cold War, submitted to the UN a draft of what would become the Chemical Weapons Convention.[104] The agreement, which was initially signed by 130 countries, was by far the most comprehensive and far-reaching of any chemical weapons agreements to date. The Convention prohibits the production and use of chemical weapons, mandates destruction of existing weapons and any production facilities, and includes a comprehensive and intrusive inspection regime.[105] Today, 188 of 196 countries recognized by the UN have become members of the Organisation for the Prohibition of Chemical Weapons (OPCW), the implementing body established by the Treaty to facilitate and ensure compliance.[106] Two of the remaining eight, Israel and Myanmar, have signed but not yet ratified the agreement. While timelines have slipped with respect to complete destruction of some stockpiles, the Convention has played a key role in the reduction of chemical weapons and near elimination of their use. Of the eight remaining countries, only one has been linked to actual deployment of chemical weapons in recent years. Recent allegations regarding the use of chemical weapons by Syria during ongoing internal conflict prompted rapid and harsh condemnation by both the

[103] Price, in fact, admits that a fear of massive retaliation seems "largely responsible for inhibiting Iraq," but again contends that even in this case, "deterrence cannot be understood without recognizing the role of a prior stigma attached to chemical weapons; this stigma set chemical weaponry apart as a symbolic threshold of acute political importance." Price, "A Genealogy of the Chemical Weapons Taboo," 77-78.

[104] Michael Bothe, Natalino Ronzitti, and Allan Rosas, *The New Chemical Weapons Convention--Implementation and Prospects* (The Hague ; Boston: Kluwer Law International, 1998), 17.

[105] Ramesh Chandra Thakur, Ere Haru, and United Nations University., *The Chemical Weapons Convention: Implementation, Challenges and Opportunities* (New York: United Nations University Press, 2006), 21.

[106] Organization for the Prohibition of Chemical Weapons, "OPCW Member States," http://www.opcw.org/about-opcw/member-states/ (accessed 25 January 2013).

OPCW and UN Secretary General.[107] As of this writing, the allegations had not been proven.

As with landmines, the emergence of a chemical weapon taboo appears to have struck a blow against a strictly determinist outlook and found room for forces of social constructivism. This case provides more historical precedent for the power of social and political construction and further strengthens the case against resignation to a technologically determined future. Technology, it appears, can be placed back in the box even after it has been opened.

Nuclear Weapons

Owing to the unique nature and global impact of nuclear weapons, as well as their recent development, their history is generally more familiar than either landmines or chemical weapons. The specter of nuclear war, after all, loomed over all but the youngest generation's head. Those born within the last twenty years may not have contemplated the horror of Mutually Assured Destruction, but anyone alive in the fifty years prior has. The depths of nuclear weapons development, therefore, need not be as exhaustively plumbed.

Countless books have been written on the subject of nuclear proliferation and, perhaps equally as interesting, non-proliferation.[108] Theories regarding proliferation range from power-based, in which proliferation and development decisions are made in the context of the pursuit of security and prestige, or lack thereof, to norm-based, which revolve around the coercive influence of international institutions and regimes.[109] Some

[107] Organization for the Prohibition of Chemical Weapons, "OPCW Statement on Alleged Chemical Weapons in Syria," http://www.opcw.org/news/article/opcw-statement-on-alleged-chemical-weapons-in-syria/ (accessed 16 April 2013).

[108] "Proliferation," as referred to throughout this thesis, refers solely to so-called horizontal proliferation (the acquisition of nuclear weapons by nonnuclear states), as opposed to vertical proliferation (the quantitative and qualitative expansion of arsenals by states already in possession of nuclear weapons). Evan S. Medeiros, *Reluctant Restraint: The Evolution of China's Nonproliferation Policies and Practices, 1980-2004*, Studies in Asian Security (Stanford, CA: Stanford University Press, 2007), 34.

[109] T.V. Paul, *Power Versus Prudence: Why Nations Forgo Nuclear Weapons* (Ithaca, NY: McGill-Queen's University Press, 2000), 6-11. One particularly illuminating theory suggests that the decision to proliferate can in fact be explained through mutual application of two variables: *Security* and *Stature*. In her doctoral dissertation, Col Suzanne "Buns" Buono suggests that through analysis of a state's "perceived level of military inviolability" (*Security*) and its "prestige, status, prominence, and integration in the international community," (*Stature*) one should observe "a clear correlation and, where applicable, covariance" between these variables and its nuclear weapons choices. Suzanne C. Buono, "Demystifying Nuclear Proliferation: Why States Do What They Do," (PhD diss., Johns Hopkins University, 2011), 77, 81, 90.

states, regardless of the power- or norm-based calculations, simply do not have the economic or intellectual capital to build "the bomb."[110] Whatever the reason, since 1945, only nine total countries have developed the capability.[111] More importantly, since 1945 none have employed it in war.

In August of 1945, the world watched the first, and so far last, employment of nuclear weapons in the history of humanity. Admittedly, in the timeline of humanity, 70 years represents a fleeting moment, but in the context of nuclear annihilation, every moment is precious. The rapid rise in capability and capacity of nuclear weapons paired with the perhaps counterintuitive lack of use offer a glimpse of a trend of the same sort revealed by landmines and chemical weapons. Despite predictions of their unchecked ascendance by a number of respected scholars and even presidents, history has indicated humanity's preference for the alternative.[112] Today, 190 countries have joined the nuclear non-proliferation Treaty, more than any other disarmament agreement in existence.[113] At the heart of the nuclear nonproliferation regime lies a simple truth: "total nuclear war is to be avoided at almost any cost" because it represents a horror unparalleled in human history.[114] Nuclear weapons offer the capacity to destroy whole societies, if not all humanity.

When Albert Einstein sent his now famous letter to President Roosevelt outlining the possibilities for nuclear weapons development, it was not without hesitation. Though he ultimately regretted sending the letter, the prospect of Hitler's Third Reich obtaining

[110] T.V. Paul's "Power Versus Prudence" and Mitchell Reiss's "Bridled Ambition" both offer compelling arguments regarding why nations forgo or constrain nuclear capabilities. Reiss's focus on the post-Cold War environment is especially compelling, as it examines choices and calculus in a non-bipolar international security setting, something not seen since the 1940s. Moreover, calculations of this period are made in the context of extant robust programs spanning the globe but also a vigorous anti-proliferation regime. The continued success of non-proliferation in an uncertain environment is further evidence of a trend away from determinist views. See Paul, *Power Versus Prudence*, 14-34. See also Mitchell Reiss, *Bridled Ambition: Why Countries Constrain Their Nuclear Capabilities* (Washington, DC: Johns Hopkins University Press, 1995), 321-33.

[111] Despite an official policy neither confirming nor denying its possession of nuclear weapons, Israel is generally believed to have "been a nuclear state for several decades." Robert S. Norris, "Israeli Nuclear Forces, 2002," *Bulletin of the Atomic Scientists* 58, no. 5 (2002): 73.

[112] T.V. Paul specifically references the pessimism of Bernard Brodie and Frederick Dunn as well as Presidents Dwight Eisenhower and John F. Kennedy. Paul, *Power Versus Prudence*, 3-4.

[113] United Nations Office for Disarmament Affairs, "Treaty on the Non-Proliferation of Nuclear Weapons," http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml (accessed 16 April 2013).

[114] Bernard Brodie, *Strategy in the Missile Age* (Santa Monica, CA: RAND Corporation, 2007), 269.

such a weapon could not be countenanced.[115] Einstein, in signing the letter, set off a chain reaction that appeared could only end in worldwide devastation. In 1939, Germany appeared poised to wreak devastation over the entire European continent. Across the Atlantic, reality began to set in and the strategy of isolationism began to crumble. Two years later, at the hands of the Japanese, it disintegrated.[116] American participation began with an attack on Pearl Harbor and ended with the annihilation of Hiroshima and Nagasaki. In the nearly seven decades hence, no nuclear weapon has been detonated in war, though this was by no means a certain future at the time. Despite these close calls, though, and in contrast to a boisterous chorus of experts proclaiming the inevitability of their future use, nuclear weapons, like chemical, were not used again.[117] Somehow, even in the tensest moments, the world has consistently managed to step back from the nuclear precipice.

Since the beginning of the atomic era, many argued that not only was the use of nuclear weapons certain, an homage to General Sibert's "no weapon goes unused" argument, but that as such, total war was an inevitability.[118] The first test of the determinist theory played out only five years after the explosion of the first atomic bombs. As tensions mounted on the Korean Peninsula, questions regarding the use of nuclear weapons became central to strategists on all sides. Contrary to what many expected, nuclear weapons were not used.[119] To be sure, they played a role. President Truman, having developed a policy dictating general (read: nuclear) war should the stakes prove vital to national security, expedited development of the next generation of nuclear weapon: the thermonuclear bomb. On November of 1952, the first device, "Mike," was detonated over an island in the Pacific. It vaporized the island.[120] Though Truman ultimately sought to keep the war limited, the world was on notice that American advancement of nuclear technologies was anything but static. When President

[115] Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (New York: Columbia University Press, 2007), 1.

[116] Waldo H. Heinrichs, *Threshold of War: Franklin D. Roosevelt and American Entry into World War Ii* (New York: Oxford University Press, 1988), 3, 6-12.

[117] Paul, *Power Versus Prudence*, 3-4.

[118] Brodie, *Strategy in the Missile Age*, 229.

[119] Paul, *Power Versus Prudence*, 3-4.

[120] Campbell Craig, *Destroying the Village: Eisenhower and Thermonuclear War* (New York: Columbia University Press, 1998), 33-37.

Eisenhower took over the Presidency in 1953, his use of "atomic diplomacy" against North Korea and China to gain political arrangements more favorable than may have otherwise been obtainable was evidence of the power nuclear weapons held over international conflict and negotiations.[121] Merely the threat of their use provided the United States with substantial bargaining power. Interestingly, at least one author has speculated that despite how Eisenhower's policy of "Massive Retaliation" was perceived at the time, he was personally against nuclear war and in fact sought to formulate a policy that would "evade" it. In this author's view, Eisenhower's policy aimed to constrain his own advisors more than it did the Soviet Union.[122] Ultimately, however, the impetus behind the strategy is immaterial. In the event, despite saber rattling and posturing on both sides, nuclear weapons were not used.

In 1962, the world watched as nuclear weapons once again moved to the fore. In October of that year, during what became known as The Cuban Missile Crisis, the United States and the Soviet Union came arguably as close as they would be to nuclear war. President John F. Kennedy himself offered a probability of disaster somewhere "between 1 out of 3 and even."[123] Despite the rhetoric on both sides, however, nuclear weapons remained holstered. The actions and negotiations of both governments were undoubtedly complex and the tensions remained extraordinarily high throughout; but in the end, the bomb dropped on 9 August 1945 would remain the last. 17 years later, the nuclear NPT was drafted. Those who agreed to it authorized the UN's International Atomic Energy Agency to begin policing member countries to prevent further proliferation of nuclear weapons.[124]

[121] Craig, *Destroying the Village*, 48.

[122] For an in depth exploration of this argument, *see Destroying the Village: Eisenhower and Thermonuclear War.* Campbell Craig makes a compelling argument that through obfuscation (he refused to be nailed down, much to the consternation of his Joint Chiefs, regarding exactly what would trigger use of nuclear weapons by the United States) and an all-or-nothing approach to war with the Soviets, he compelled his advisors to favor negotiation over escalation. Eisenhower was convinced that any conflict with the Soviet Union would lead to all-out nuclear warfare and worried that his own advisors would make strategic miscalculations that might lead to annihilation of both sides. According to Craig, Eisenhower used this strategy to successfully "evade" nuclear war. Craig, *Destroying the Village*.

[123] Graham T. Allison, "Conceptual Models and the Cuban Missile Crisis," *The American Political Science Review* 63, no. 3 (1969): 689.

[124] George Bunn, "The Nuclear Nonproliferation Treaty: History and Current Problems," *Arms Control Today* 33, no. 10 (2003), http://search.proquest.com/docview/211242485?accountid=4332.

The path to the NPT began with the opening of the 18-nation Disarmament Conference in March of 1962. Negotiations between the two primary parties, the United States and the Soviet Union, progressed steadily over the next six years. China and France chose not to participate and instead successfully pursued their own nuclear weapons programs. China's decision to opt out had a domino effect that, though limited, negatively impacted development of the agreement. China's absence led India, who had actively participated in the negotiations but who also had an antagonistic relationship with China, to ultimately refuse to sign. This caused Pakistan, another Indian adversary, to withdraw its support. Separately, though the United States had attempted to restrain Israel's nuclear ambitions, they, too, refused to join the Treaty. China and France were later permitted to join the Treaty under the same provisions as the original three nuclear-weapons states (the United States, Soviet Union, and United Kingdom). India and Pakistan never have signed the Treaty and both eventually acquired their own nuclear weapons. Israel is widely believed to possess their own as well.[125]

While the NPT was not fully successful in preventing the proliferation of nuclear weapons, it must be regarded as largely successful given the number of eventual signatories and relative restriction of nuclear proliferation. More importantly, the Treaty is a reflection of an international norm. Additionally, the Treaty's role in the nuclear landscape strengthens the nonproliferation regime and has had at least some persuasive effect on state behavior. In many cases, it figured prominently in states' nonproliferation decisions.[126] Some point to the fact that Iran is widely suspected of pursuing its own weapons program. Further, North Korea withdrew from the Treaty in 2003, the first, and so far only, state to do so in the Treaty's 45-year history. Be that as it may, nuclear weapons have not permeated warfare to the extent that many in the Atomic Age predicted they would. In the nearly seven decades since Fat Man and Little Boy were dropped over Japan, the specter of warfare involving nuclear weapons has arguably declined. The arms race between the two superpowers of the Cold War was run at a breakneck pace, with more than 32,000 warheads in the US inventory alone in 1967.[127] Since that time,

[125] Bunn, "The Nuclear Nonproliferation Treaty: History and Current Problems."

[126] Reiss, *Bridled Ambition,* 331.

[127] Thomas B. Cochran, William M. Arkin, Milton M. Hoenig, and Natural Resources Defense Council., *Nuclear Weapons Databook* (Cambridge, MA: Ballinger Pub. Co., 1984), 12.

however, the number of weapons in both countries has declined significantly. Today, the two largest stockpiles belong to the United States, with an estimated 4,950 warheads,[128] and Russia, with an estimated 4,430.[129] The United States and Russia continue to work to reduce their own stockpiles of weapons and both weigh heavily any introduction of nuclear-related technologies that introduce uncertainty or imbalance.[130] Much like chemical weapons, a taboo exists vis-à-vis nuclear weapons, one that has grown as the technology has matured and societies have come to grips with the horror it is capable of producing.[131]

Though there is admittedly no guarantee regarding the future of nuclear weapons, the historical record suggests there exists a very high bar for their use. Nuclear devastation appears unlikely, at least in the foreseeable future. The world has undergone significant change in the years since the United States ushered it in to the atomic age. The international stage has gone from multipolar to bipolar to unipolar and, perhaps, will return to multipolar once again in the near future. Throughout all of these changes, amid the tension and uncertainty of major shifts in the geostrategic landscape, nuclear capabilities have remained ultimately idle. Contrary to popular belief, the world has yet to undergo nuclear Armageddon. Moreover, it has seen exactly zero uses of nuclear weapons since the nuclear NPT. In the case of nuclear weapons, the world has made every effort to reseal the lid on their use in future warfare.

Conclusion: Closing Pandora's Box

According to Greek mythology, after Pandora opened her box, all evil escaped into the world, never to be caught. She hurried to close it, but it was of no use. All of the contents had escaped. This much of Pandora's story is well known and often referenced

[128] Up to 3,000 additional warheads have been retired and await dismantlement. Hans M. Kristensen and Robert S. Norris, "US Nuclear Forces, 2012," *Bulletin of the Atomic Scientists* 68, no. 3 (2012): 84-85.

[129] Up to 5,500 additional warheads have been retired and "may be waiting dismantlement…" Hans M. Kristensen and Robert S. Norris, "Russian Nuclear Forces, 2012," *Bulletin of the Atomic Scientists* 68, no. 2 (2012): 88.

[130] Reiss, *Bridled Ambition*, 322.

[131] Reiss opines that the end of the Cold War has strengthened the taboo and further suggests that the taboo itself may have hastened the collapse of the Soviet Union in the first place. Reiss, *Bridled Ambition*, 2. Mueller contends that after Hiroshima and Nagasaki, many came to view nuclear weapons as akin to chemical weapons. The drawn-out deaths and radiation poison, burns, and long-term damage caused by nuclear weapons, similar to killing with gas, is somehow less moral than traditional methods of killing with bullets and shrapnel. John E. Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda* (New York: Oxford University Press, 2010), 61-63.

in Western culture. It is not, however, the whole story. In the ancient poem of Hesiod, one thing remained in Pandora's jar: Elpis, the spirit of hope.[132] Today, with the benefit of hindsight, it is apparent that there is hope for recapturing some of the evil that has escaped into the world. Though mankind was not wholly successful shielding non-combatants from the unintended consequences of left-over landmines nor from the horrors of poison gas or nuclear weapons, it appears the lid has been, to some extent, tamped back down on these weapons. While the reasons behind such constraint are as numerous as the countries who have agreed to abide by them, the simple fact is that, despite predictions to the contrary, the footprints of all three forms of weapons–landmines, chemical weapons, and nuclear weapons–have declined as regimes aimed at curtailing their use have grown and solidified world opinion against them.

Between the three categories of weapons, all but one country (Israel) has voluntarily limited the use of at least one of them, and in many cases, all three.[133] The class with the most non-signatories (though at 161 out of 196 countries, the ratio is still very high), landmines, are also the most complex with regard to form and function. Additionally, the prospect for a full ban must contend with the fact that in a number of locations, they are perceived as vital to a country's self-defense. Chemical weapons, too, represent a strong case for a trend toward discrimination; despite their widespread use only two decades prior, they were never used during World War II. Indeed, lethal chemical weapons have only been confirmed as having been used twice since the close of World War I. This despite what many predicted would be a new way of war. Finally, nuclear weapons reflect perhaps the strongest historical proof of the prospect for containing and constraining a weapon technology even after first use. Since, 1945, not one nuclear weapon has been used and, while not perfect, the track record for nonproliferation is arguably the best in all of human history, especially given the power and prestige afforded those who would obtain such weapons. Though reasons arguably

[132] The Internet Sacred Text Archive, "Hesiod: Works And Days," http://www.sacred-texts.com/cla/hesiod/works.htm (accessed 29 January 2013).

[133] Israel is the only country to not formally limit use of landmines, chemical, or nuclear weapons. Israel has signed the Chemical Weapons Convention, but has not yet ratified it. Organization for the Prohibition of Chemical Weapons, "Non-Member States," http://www.opcw.org/about-opcw/non-member-states/ (accessed 25 January 2013).

vary from altruistic to pragmatic, the fact that so many nations have chosen to constrain the use of a given class of weapons is important.

Again, the key is not how binding the agreements themselves are. In the anarchy of international order, it would be naïve to consider any agreement fully compulsory. Any state may break any agreement at any time if it so chooses. The prospects for punishment are ad-hoc, if they exist at all. This is beside the point, though. The importance of these agreements lies in the norms they reflect and strengthen. Institutions "raise the costs of sharp reversals in policy and create vested political interests and organizational inertia that reinforce stable and continuous relations."[134] In an anarchical system, credibility is critical and compliance with international norms and agreements is one essential way to establish and build such credibility.[135] Regardless of the motivating factors, the fact remains that states *do* agree to limit use of types of weapons, and they do so often out of a concern for a lack of discrimination.

The world has seen that once opened, Pandora's Box can sometimes be closed again, or at least somewhat resealed. This is especially true of indiscriminate weapons which inflict a high proportion of negative effects on civilians and non-combatants. There is no invisible force propelling weapons toward greater and greater destruction and no predetermined path toward increased adverse effects on civilians. The determinist view of weapons development and usage, particularly in the context of discrimination concerns and trepidation over collateral damage, is less than certain.

[134] Ikenberry, *After Victory*, 65.

[135] Thomas Schelling explores the concept of credibility in the international system at length throughout this seminal work. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008).

Chapter 3

Hitting Undo: Prospects for an Indeterminate Future

According to Lynn White, a prominent technological historian, as mankind's understanding of technological development has grown, it has become clear that "a new device merely opens a door; it does not compel one to enter."[1] In other words, technology itself does not induce exploitation for one end or another; it merely offers an opportunity which must be acted upon by man. Admittedly, the existence of a given technology may powerfully influence man's desires. The airplane, for instance, certainly inspired more men and women to fly than would have otherwise taken to the air had it remained but a figment of science fiction. The tenor of today's cyber discussion, however, ascribes to cyberspace something more than influence. In the eyes of many, as cyberspace has become ever more intertwined with societies and, perhaps more importantly, warfare, it has taken on a momentum of its own, hurtling man ever closer to the edge of complete cataclysm. This deterministic view envisions the nature of cyberspace as inherently powerful enough to launch mankind through the door of mass destruction, discounting the prospect of restraint. In much of the contemporary literature, there is an inordinate focus on risk, so much so that it threatens to drown out voices calling for a balanced discussion of the most salient aspects of cyberspace. Worse, those who deign to counter the paranoia often posit a converse argument that focuses narrowly on undermining cyber power's perceived revolutionary nature and, in so doing, simply skews to the opposite end of the spectrum. Both arguments are excessively obtuse. An accurate analysis of the prospects for cyberspace necessitates a more nuanced approach. True perception requires piercing the rhetoric of revolution while taking care not to be seduced by cynicism.

Discussions regarding cyberspace often devolve quickly into a debate of extremes, with one side excoriating society and the government for turning a blind eye to the risks and ongoing revolution in cyberspace, and the other scoffing the so-called cyber prophets as just the latest in a long line of technological doomsday-lovers, proclaiming

[1] Lynn Townsend White, *Medieval Technology and Social Change* (Oxford, UK: Clarendon Press, 1962), 28.

the impending doom of the newest virtual apocalypse.[2] Productive debates are often hung up on endless wrangling over whether it is a warfighting domain or if a cyber attack could ever constitute an act of war. These debates, while helpful to establish a common lexicon, often obscure the more germane issues and mire discussion in a debate over semantics. Worse, these sorts of meandering discussions over word choice often result in overreliance on false or misleading comparisons and analogies, grasped at in an attempt to bring clarity and familiarity to an often disordered and strange new world. Pursuit of definitional consensus takes precedent over true insight. Becoming bogged down in these sorts of deliberations obscures and sidelines otherwise productive analysis of the salient and unique aspects of cyberspace and operations within it. To the extent that such discussion leads "strategists and operators to presumptions or conclusions that are not derived from observation and experience, [such] characterization may well mislead."[3] Closer inspection reveals that many issues in the cyber realm are not as vexing as they appear at first glance.

Cyberspace is new and unusual, but it is not inherently evil. The current geopolitical environment and some unique aspects of cyberspace combine to create a compelling, if misguided sense of inevitability. Contrary to the gospel of determinism, cyberspace is not unavoidably destined for Armageddon; the path toward wanton digital destruction is not preordained. Closer examination reveals prospects for a sunnier future, at least one characterized less by civilian torment and more by mutual constraint, if not full cooperation. Much of what is portrayed as destruction turns out, upon closer inspection, to be better characterized as distraction or disruption, still not desired, but preferable to complete devastation. Additionally, though warfare of the twenty-first century may differ greatly in terms of technology used to pursue it, the nature of war remains unchanged, even in the revolutionary realm of cyberspace: war, even prosecuted in cyberspace, still serves a political function and, as such, is subject to a number of factors outside of digital ones and zeroes. One aspect of cyberspace, its potential for hyper-precise targeting of enemy capabilities, may actually lead to an increase in discrimination, rather than the oft-projected slide toward civilian targeting. The

[2] Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011), 208.
[3] Martin C Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8 (2012): 322.

prospects for restraint in cyberspace are, though nascent, plausible. History has demonstrated an international preference for discrimination in warfare. While one cannot be certain cyber Armageddon will not one day arrive, neither can he be sure it will. In an effort to counterbalance the prevailing pessimism in cyberspace as evidenced in chapter 1, it is important to examine what leads to the sense of panic and offer a possible alternative future.

Why Worry? Sources of Panic in Cyberspace

Cyberspace is not the first so-called revolutionary technology to enter the pantheon of modern warfare. Man has always struggled for an edge in the pursuit of survival; the exploitation of cyberspace is merely the latest reflection of this struggle. Nor are operations by, with, and through cyberspace the first to be touted as revolutionary, certain to change the nature of conflict or threaten mankind to an extent as yet unparalleled. 100 years ago, chemical weapons were expected to alter forever the face of warfare.[4] 50 years later, the prospect of nuclear warfare was nearly universally expected.[5] Yet in both cases, use of such weapons was, and remains, significantly constrained. Why, then, in the face of such evidence, do predictions remain dour? The answer is twofold, consisting of both external and internal factors. First, the time is ripe for anxiety. As the next section shows, history has demonstrated that shifts in the geostrategic landscape that coincide with the introduction of new technology tend to induce apprehension. Secondly, cyberspace's unique aspects of ubiquity, speed, anonymity, and heightened civilian vulnerability exacerbate the already nascent prospect for fear. The tale of cyber Armageddon is, therefore, internal and external, but it begins on the international stage.

Geopolitical Change and New Tech: A Recipe for (Misguided?) Restlessness

The uncertainty that characterizes today's international security environment is not a new phenomenon. Nor is its combination with new and wondrous warfighting capabilities. In the last century alone, the introduction of air and nuclear power during times of geopolitical upheaval inspired fear and predictions of an inevitable descent into

[4] Amos A. Fries and Clarence J. West, *Chemical Warfare* (New York: McGraw-Hill Book Company, inc., 1921), http://books.google.com/books/reader?id=kGGpuj9s-tIC&printsec=frontcover&output=reader&pg=GBS.PR2, ix.

[5] T.V. Paul, *Power Versus Prudence: Why Nations Forgo Nuclear Weapons* (Ithaca, NY: McGill-Queen's University Press, 2000), 3-4.

technology-induced cataclysm.[6] In times of uncertainty, it is natural to reach into the past in an effort to distill clarity from complexity. In so doing, however, it is imperative that one not overlook key differences and exaggerate similarities. Today's shifting geopolitical environment is driving an overreliance on analogies that while potentially instructive, when combined with the uncertainty of cyberspace, have led to some tenuous conclusions and an overall sense of inevitable cataclysmic conflict in cyberspace. As opposed to the inherent aspects of cyberspace addressed in the next section, these concerns may be based more on sweeping generalizations and false analogies than truth. While cyberspace itself poses valid concerns that must be faced, a significant source of apprehension stems from well-meaning but clumsy attempts to liken the challenges of today to those faced (and overcome) by the country's forefathers.

What's Old is New Again. At the turn of the twentieth century, the invention of the airplane and, in particular, its introduction into military service during World War I appeared to many to signal a revolution in warfare. To Giulio Douhet, a leading air power theorist at the time, command of the air was both necessary and sufficient to achieve victory in war.[7] In Douhet's estimation, nothing on the ground would ever stop air power from reaching its objective.[8] Douhet's oft-referenced contemporary, Billy Mitchell, echoed Douhet's enthusiasm. Mitchell believed the advent of air power necessitated a complete rewrite of both the rules and strategies of warfare, asserting that "[t]he uses of aircraft in warfare would then be limited only by the inability of human ingenuity to conceive further uses for this new agency of destruction."[9] Air power had come to the fore in the midst of an upheaval in the international order. World War I offered a glimpse of its potential. Soon after Douhet and Mitchell penned these words, the world found itself embroiled in yet another conflagration that would eventually encompass the entire globe. At the close of World War II, nuclear weapons took a similar spot at the center of significant international upheaval. Having shut the door on

[6] General Billy Mitchell often extolled the virtues of air power and suggested that its introduction to the battlefield was limited only by the creativity of the individual human mind. William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009), 243. As for nuclear weapons, intellectuals and politicians alike warned of the inevitable downward spiral into mass destruction. Paul, *Power Versus Prudence*, 3-4.
[7] Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 1998), 25.
[8] Douhet, *The Command of the Air*, 9.
[9] Mitchell, *Winged Defense*, 6, 243.

one international order, they created the foundation for a new one. Many at the time believed that this new technology would alter warfare forever. While nuclear weapons have undoubtedly played a defining role in international relations over the last seven decades, however, mankind has thankfully never witnessed the “nuclear battlefield” that many asserted would emerge.

Cyber power is coming of age in a similar era of transition. The Berlin Wall fell only eight months after Tim Berners-Lee first authored his proposal for the World Wide Web;[10] the first web server came on line seven months after the dissolution of the Soviet Union.[11] Cyberspace emerged in an historical era [in which] the West perceived its dominance to be fading.[12] It established its bonafides as the world shifted from bi- to unipolarity and became a full-fledged force as the unipolar order began to show cracks in its own foundation. The introduction of a groundbreaking technology in the midst of such upheaval is bound to have a dramatic effect. Simply put, a tendency toward hyperbole exists because the timing is ripe for it.

Today, as cyberspace continues to permeate all aspects of society, many grasp for something familiar in pursuit of understanding and explanation. Two decades after the World Wide Web was invented, the world’s knowledge can be carried on a smartphone in one’s pocket. Furthermore, the specter of a multipolar world looms large, potentially inducing anxiety for some (those holding the most power in the current geopolitical landscape) and reflecting an asymmetric opportunity for others (those who would challenge the status quo).[13] In the midst of increased international uncertainty, a technology as potentially disruptive (both positively and negatively) as cyberspace only compounds the situation. In such an environment, societies understandably search for analogies in an attempt to better understand their surroundings. This is true both from an international security perspective and a technological one. As both are intertwined in reality, the analogies used tend to be as well.

[10] Tim Berners-Lee, "Information Management," (Proposal submitted to CERN, 1989), 1.
[11] British Broadcasting Coroporation, "How the Web Went World Wide," http://news.bbc.co.uk/2/hi/technology/5242252.stm (accessed 24 March 2013).
[12] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London, UK: The International Institute for Strategic Studies, 2011), 128.
[13] Samuel P. Huntington, "The Lonely Superpower," *Foreign Affairs* 78, no. 2 (1999): 37, 49.

In Search of Simplicity. US foreign policy of the early twenty-first century has displayed a clear yearning for the simpler times of the Cold War. As the world transitioned from the clear-cut bipolarity that dominated the latter half of the twentieth Century into the more complex and uncertain structure of the early twenty-first, the United States caught a fleeting glimpse of what could have been. The world stage of the 1990s appeared to be one building toward the panacea of peace (at least from an American perspective) where the United States played the role of heroic cowboy, poised at a moment's notice to intervene on behalf of the downtrodden and ready to fight in the face of evil.[14] Brief forays into complexity notwithstanding (Somalia, the Balkans, etc.), it appeared the United States wielded the power necessary to provide order to the anarchical international system. As the turn of the century passed, however, it became clear that the complexity of Somalia and the Balkans would characterize the norm rather than the exception.

If the US of 10 September 2001 had glimpsed hegemony, the paradigm was violently altered the next day. What once was hidden suddenly gained very sharp focus and it directly opposed the worldview held by many in the United States. Thomas Kuhn, a prominent physicist and historian, suggested that, "[l]ike a gestalt switch," a revolution in paradigm "must occur all at once."[15] On 11 September, it became clear that the paradigm of the last decade had restricted many decision-makers' views. The path toward hegemony was not as straight as it may have seemed in the immediate aftermath of the Cold War. As the United States shifted to confront this new reality, it became clear the world would not march obediently to the sound of American bugles.[16] In the face of uncertainty, some foreign policy experts contend, the US foreign policy began to

[14] Barry Posen, a security studies expert, uses the term "primacy" to describe the policy widely ascribed to in the 1990s to describe a sort of benevolent hegemony that preserved American power and freedom of action, but through a more multilateral and liberal strategy, especially during the Clinton administration. Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (2003): 5-6.

[15] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago, IL: University of Chicago Press, 1996), 151.

[16] Despite optimistic views of future US freedom of action in the 1990s, the following decade made it clear that despite possessing a significant conventional advantage, challenges remained to US dominance. Alluding to these challenges, Posen described the existence of "contested zones," where, despite US dominance of the commons, "a combination of political, physical and technological facts…combine to create…arenas of conventional combat where weak adversaries have a good chance of doing real damage to U.S. forces." Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," 22.

search for what it knew: an enemy.[17] The fact that China happened to a communist country, just like the last major US adversary, appeared to make the analogy an even better fit. This search has had the dangerous consequence of oversimplifying foreign and defense policy as well as prospects for cyberspace.

The combination of growing ambiguity vis-à-vis the world order and increasing rate of change has driven the West, and especially the United States, to reach into the past to explain the present and make sense of the future.[18] The US “pivot to the Pacific,” a popular euphemism for the recent shift in US strategic focus from the Middle East to East Asia, is doubtless a welcome reprieve for many in the American government tiring of the complexity and ambiguity of purpose of the Middle East. Many, in fact, see the shift as a return to the same sort of containment policy enacted throughout the Cold War, except this time aimed at China.[19] The logic is appealing: As the Soviet Union reached nuclear parity with the United States in the 1950s, China is the popular face of threats in cyberspace. China is the country often on the lips of senior government officials describing the cyber threat to national infrastructure and military systems. And with good reason: it was two Chinese army colonels, after all, who wrote over a decade ago

[17] Paul Kennedy, an international relations and grand strategy expert, detected a “sense of nostalgia” for the “familiar contours of that bygone conflict” in the face of a murkier and more complex present. Paul Kennedy, "The Good Old Days of the Cold War," *Los Angeles Times* (2007), http://www.latimes.com/news/la-op-kennedy18feb18,0,6800641.story. Marvin Kalb, of the Brookings Institute, warned again in 2012 of the dangers of making comparisons between China and the Soviet Union, suggesting that “[i]f you listen to official Washington-and not just the politicians on the right and left-but also the think tank analysts and the media, you might well conclude that
China has replaced the old Soviet Union as the bulky, powerful adversary challenging America’s central place in the world…” Marvin Kalb, "China Is Not the Soviet Union," *Up Front* (2012), http://www.brookings.edu/blogs/up-front/posts/2012/01/10-china-kalb. Joseph Nye, a professor at the Harvard Kennedy School and former Pentagon official, warned again of an American foreign policy that smacks of the same containment strategy used against the Soviets during the Cold War. Joseph Nye, "Work with China, Don't Contain It," *The New York Times* (2013), http://www.nytimes.com/2013/01/26/opinion/work-with-china-dont-contain-it.html.

[18] David Rothkopf , Chief Executive Officer and Editor-at-Large of *Foreign Policy*, contends that since the end of the Cold War, the United States has been in search of an enemy for a number of reasons, not the least of which is that it is much easier to characterize a threat and conceptualize a cause *against* something concrete. He asserts that, especially in the context of the waning wars spawned in the wake of 11 September 2001, the specter of a rising China provides a useful foil for politicians looking to coalesce public support. While cynical in tone, the underlying premise is valid. Simply put, foreign policy is theoretically simplified (or at least more easily articulated and argued for) when an enemy can at least be identified and strategies proposed to protect the country and mitigate (real or perceived) threats. David Rothkopf, "The Enemy Within," *Foreign Policy*, no. 193 (2012): 1-2.

[19] The Foreign Policy Initiative, "The Obama Administration's Pivot to Asia: A Conversation with Assistant Secretary Kurt Campbell, Moderated by Robert Kagan, transcript," http://www.foreignpolicyi.org/files/uploads/images/Asia%20Pivot.pdf (accessed 20 March 2013).

about the promise of cyber operations to provide asymmetric capabilities to counter the seeming insurmountable conventional power of the United States.[20] Furthermore, the sheer size and scope of the Chinese cyber espionage effort provides for a convincing villain. Experts estimate that just one of the more than 20 dedicated Chinese cyber espionage units is responsible for the theft of hundreds of terabytes of data from at least 141 organizations spanning 20 major industries.[21] China is the foil of first resort for hypothetical future wars in cyberspace.[22] That China is the cyber adversary is old news. It has become cliché to blame the Chinese for all problems cyber.[23]

China represents a perfect target for Western anxiety: its prestige and economic clout is on the rise and it represents everything the West fears about an uncertain cyber future. To shift focus to China is to kill two proverbial policy birds with one stone: keep China in check and the status quo is maintained while simultaneously mitigating the apparent primary risk in cyberspace. The fear over uncertainty on the international stage

[20] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 50-52.
[21] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (2013).
[22] Even as he cautions against a clunky view of China's national objectives, Joel Brenner dedicates a full chapter of his most recent book to suggesting a hypothetical scenario in which China plays the role of principal adversary. Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 137-56.
[23] Statements by key government officials regarding cyberspace often make their way into Chinese territory. As recently as March 2013, Gen Keith Alexander, current head of the National Security Agency as well as US Cyber Command, and Lt Gen James Clapper, USAF, retired, current Director of National Intelligence, both referred to China during congressional testimony regarding US cyberspace capabilities and threats. General Alexander often includes China in discussions of how the United States will combat threats from cyber espionage. Mark Mazetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate against Cyberattacks," *The New York Times* (2013), http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all&_r=0. A day prior, White House National Security Advisor Tom Donilon decried cybersecurity threats emanating from China "on 'an unprecedented scale'" and warned that, if not controlled, they could weaken the economic relationship between the two countries. Andrew Rafferty, "Cybersecurity Threatens US-China Relationship, White House Official Says," *NBCNEWS.com* (2013), http://usnews.nbcnews.com/_news/2013/03/11/17273068-cybersecurity-threatens-us-china-relationship-white-house-official-says?lite. Contemporary cyberspace literature is rife with references to China as either *the* or at least *a* major threat to US cybersecurity. S. Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009), 10, 66. See also David Sanger's hypothetical cyberattack scenario. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 1st ed. (New York: Crown Publishers, 2012), 266. See also Joel Brenner's hypothetical cyberattack. J. Brenner, *America the Vulnerable*, 137-56. Of course, one cannot deny that China as undertaken considerable efforts to exploit vulnerabilities in cyberspace to conduct espionage against the United States, but the true nature of the threat risks being drowned out in the cacophony of alarm bells regarding the perceived threat such espionage portends. Additionally, the China-as-cyberbogeyman scenario vastly oversimplifies the geostrategic and security landscape in cyberspace and downplays the impact and import of other actors and issues.

and the cyberspace domain is thusly quelled. The United States has come to rest in a new paradigm built on an analogy that, while useful, may blind policymakers to important aspects of the shifting international order and more nuanced aspects of the challenges of cyberspace. Furthermore, it conflates the challenge of a rising China with the perceived threat of pending doom in cyberspace, stoking the fires of the determinist predictions of looming cyber apocalypse. In fact, closer examination reveals several weaknesses in this back-to-the-future analysis.

Cracks in the Comparison: China's no Russia. First, the West's relationship with China is not nearly so straightforward as this sort of analysis implies. As opposed to the Soviet Union of the Cold War, China is tightly integrated with economies across the globe; according to at least one report, China is the biggest trading nation in the world.[24] The country that threatens to steal technological secrets and undermine national security objectives through cyberspace is the same one that underpins a significant portion of the world economy. Whereas the Chinese are comfortable existing within a spectrum of mutual benefit *and* confrontation, the West, and Americans specifically, often have trouble operating within that sort of ambiguity. China's primary strategic objectives consist of increasing its citizens' standard of living and re-establishing a prominent place in the international order. By themselves, these objectives do not make China the mortal enemy of the West.[25] The neo-realist argument of zero-sum power struggles notwithstanding, the West can continue maintain prestige as China works to gain a new foothold on the international stage. The Cold War comparison to the Soviet Union is useful only insofar as it speaks to some *possible* prospects for a rising peer competitor. However, the West must not settle for a strategy based on broad brushstroke comparisons; the approach toward China, and indeed all rising powers, must be predicated on "subtler terms than the convenient black-and-white simplicities of ally and foe."[26]

Uncertainty on the world stage and within the realm of technological development has driven a yearning for a time when the enemy was easy to identify and national

[24] Bloomberg, "China Eclipses U.S. as Biggest Trading Nation," http://www.bloomberg.com/news/2013-02-09/china-passes-u-s-to-become-the-world-s-biggest-trading-nation.html (accessed 1 May 2013).
[25] J. Brenner, *America the Vulnerable*, 67-69.
[26] J. Brenner, *America the Vulnerable*, 67.

interests were clearly articulated. The West must not allow that yearning to become overly reliant on only partially applicable metaphors lest they crowd out consideration of strategic opportunities and portray the emergence of cyberspace alongside the emergence of new, more powerful actors on the world stage as a one-way ticket to conflict.

Mistaken Metaphors: Cyberspace Defies Simple Comparison. Weak analogies do not stop at the international border. Change tends to produce anxiety, and nowhere is change more prevalent than in the lives of twenty-first century westerners who, in the space of only 20 years, have gone from floppy discs to smartphones. The pace of technological evolution is nearly inconceivable. In an effort to distill clarity in a rapidly changing technological environment, many have gravitated toward analogies that appear to simplify otherwise complex challenges. Former Secretary of State Hilary Clinton, for instance, has described some countries' online censorship as an "information curtain" and likened the digital divide between free and suppressed peoples to the Berlin Wall that came to symbolize the same separation in the physical realm of the Cold War.[27] Comparisons such as these provide comfort; in time of uncertainty, leaders often seek the solace of metaphor. Unfortunately, this particular metaphor, one of cold warriors fighting existential battles of black-and-white ideology, tends to do as much harm as good.

Painting the challenges of cyberspace in the colors of the Cold War ascribes to it a level of existential threat that tends to induce delusions of both grandeur and panic. Writers warn of the dastardly designs of their nations' enemies, spinning tales of unfettered destruction against a the backdrop of an era that was shot through with fear of nuclear annihilation. In this telling, the internet becomes a place of foreboding intrigue where devastation can be unleashed with the press of a button. While metaphors and models are undoubtedly helpful when attempting to untangle and conceptualize the daunting strategic landscape of cyberspace, comparisons carry with them an inherent risk of overreach. According to Keith Shimko, a political psychologist, "people often move from the identification of similarities to the assumption of identity – that is, they move from the realization that something is *like* something else to assuming that something is

[27] Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom" (address, The Newseum, Washington, DC, 21 January 2010).

exactly like something else."[28] American politicians have been particularly prone to this sort of overreach in the realm of cyberspace, often invoking success in the Cold War as blueprint for success in a so-called cyber war.[29]

The comparison is alluring. It offers the dual ability to at once make cyberspace *and* the future international security situation understandable and predictable. Here is where the comparison becomes most dangerous. In likening the emerging problems of cyberspace to those faced on the international stage throughout the second half of the twentieth century, many begin to see cyberspace as inherently a battlespace. Certainly, potential exists for conflict in the domain. The comparison, however, carries with it a high risk of oversimplification and fallacious conclusions about the intrinsic nature of cyberspace and operations within it. Yuen Foong Khong, a professor of international relations at the University of Oxford, cautions that the very process of analogical reasoning presents inherent challenges to its application. Specifically, his research suggests that "people tend to access analogies on the basis of surface similarities."[30] Accessing the analogy allows the perceiver to go beyond the information given, leads to perseverance and, ultimately, leads "to simplistic and mistaken interpretations of incoming stimuli."[31] This dovetails with Robert Jervis's assertion that a human tendency toward consistency often leads to neglect (consciously or not) of stimuli that do not fit pre-existing notions.[32] Analogies, then, and analogical reasoning, carry with them certain inherent risks that the imprudent decision-maker may fall prey to. Indeed, in the case of cyberspace analysis, many demonstrate an inability to grasp a central tenant of analogical reasoning: "while capable of creating valuable insights…a metaphor [also] becomes a way of *not* seeing."[33] Metaphors "often create an illusion of complete intellectual mastery."[34] In an effort to make visible the contours of cyberspace, many search in vain

[28] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), 43.
[29] Morozov, *The Net Delusion*, 40.
[30] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ: Princeton University Press, 1992), 14.
[31] Khong, *Analogies at War*, 14.
[32] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 117.
[33] Gareth Morgan, *Images of Organization*, Updated ed. (Thousand Oaks, CA: Sage Publications, 2006), 5.
[34] Morozov, *The Net Delusion*, 43.

for a single lens that will distill clarity. The sophistication and complexity inherent in cyberspace will not be tamed through lessons of analogy or metaphor alone.

The time is ripe for panic. The 1930s had the airplane, the 1950s had nuclear weapons, and now the 2000s have cyberspace. In each period, an environment of uncertainty on the world stage combined with a rapid growth in a never-before seen technology to create an unease that manifested itself in dire predictions for the future. Today, cyberspace enables robot planes to drop bombs on terrorists in the remote mountains of Pakistan. The same electronic paths used for global destruction also facilitate financial transactions, control power grids, and deliver funny cat videos to millions every day. Perhaps an overanxious desire to find clarity and understanding through comparison and derived similarities can be forgiven. Forgiveness does not, however, imply acquiescence. Additional investigation into the unique nature of cyberspace must constantly be undertaken and additional analogies must be sought in pursuit of further illumination. Overindulgence in singular analogies threatens to obscure that which is often at the root of much anxiety regarding the future of cyberspace and its threat to national sovereignty.

Cyber panic, however, is not the result of timing alone. Cyberspace, and operations through it, possess unique aspects of their own, many of which are at the heart of dire predictions of destruction. These unique aspects form the foundation upon which many build their pessimistic vision of the future. While they are undeniable characteristics of this new medium, it is important to remember that they are only characteristics. They do not drive action, merely enable it. In an effort to better understand those aspects of cyberspace that inspire dire predictions of the future, further examination is necessary.

Information Change: Cyberspace's Intimidating Nature

Some aspects of cyberspace simply are intimidating. They play on man's natural tendency to fear the unknown and different. Change is scary. A fundamental discomfort with change may be the closest the human race ever comes to a universal truth. New terror often accompanies new environments.[35] Quite simply, man is most comfortable with what he knows and change threatens cognition. Today, technology is the currency

[35] Betz and Stevens, *Cyberspace and the State*, 12.

of change and its presence is overwhelming. Preeminent futurist Ray Kurzweil, in fact, argues that technology is nothing less than "evolution by other means."[36] Furthermore, he argues, the rate of evolution (change) is accelerating rapidly. Kurzweil describes an evolutionary environment that is growing exponentially, each step forward in itself enabling evolution to accelerate.[37] Writing in 1999, Kurzweil predicted that computers would achieve parity with the human brain by 2020.[38] Whether or not this prophecy holds true, the rapidity of technological change is undeniable. Today's teenagers carry around more computing power in their pockets (in the form of a phone, no less) than all of NASA possessed just a few decades ago, and they were able to harness that computing power to put men on the moon.[39] Certainly, change at this pace is likely to ruffle a few feathers, perhaps even engender a bit of paranoia. The effect is even more pronounced in that unique slice of technology referred to as cyberspace.

Cyberspace is a new medium. Though definitional debates often revolve around semantic arguments regarding the ubiquitous and eternal nature of the electromagnetic spectrum, humans have only recently harnessed it to the extent that it can be described as a "place." Cyberspace is new, and as such, can be intimidating, especially given its rate of rapid growth. To make matters worse, it is not easy to conceptualize. One can understand (and see) improvements in technology of flight. Planes with jet engines generally move faster than those with propellers. One need not understand how a jet

[36] Ray Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence* (New York: Viking, 1999), 14.

[37] Kurzweil makes a very compelling case that Moore's Law, which states that computing speed will double roughly every 18 months, is nothing more than a reflection of the "Law of Accelerating Returns," which predicts that as order increases, "the time interval between salient events grows shorter as time passes." Furthermore, since "[c]omputation is the essence of order," evolutionary "salient events" will rapidly increase in periodicity nearly ad infinitum. "Ultimately, the innovation needed for further turns of the screw will come from the machines themselves." Kurzweil, *The Age of Spiritual Machines*, 30-35. While this may seem far-fetched, it is undeniable that simple increases in computing power have allowed humans to overcome many heretofore insurmountable barriers. Computers help humans solve problems. One's definition of innovation may be inherently affected by the increased presence of technology itself. The concept of computer-innovation may simply be evolving along with technology's own growth, shifting the bar ever so slightly higher as the seemingly unobtainable is reached. Alan Turing suggested "that machine intelligence would become so pervasive, so comfortable, and so well integrated into our information-based economy that people would fail to even notice it." Kurzweil, *The Age of Spiritual Machines*, 71. Perhaps technological evolution is moving at such a break-neck pace that humans are no longer capable of easily discerning truly revolutionary break-throughs.

[38] Kurzweil, *The Age of Spiritual Machines*, 3.

[39] Michio Kaku, *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100*, 1st ed. (New York: Doubleday, 2011), 21.

engine works to comprehend its relative value over spinning rotors. Nor must one perceive the inner workings of robotic assembly to understand how it could improve the manufacture of the car he drives to work. Cyberspace, however, is different. It is a land of photons and electrons. In cyberspace, information, transactions, and most importantly, effects, can move literally at the speed of light. That teenager pulls his phone out of his pocket and magically he has a satellite image of the closest McDonald's at his fingertips along with directions, and a menu. All of this information appears nearly instantaneously out of thin air. Cyber operations are visible only through their results. In many cases, it is not even apparent that operations in cyberspace are to blame. In Iran, for instance, it apparently took years to discover that *Stuxnet* was the root of their enrichment problems.[40] Even then, it was only because a commercial computer security firm alerted them to its presence after a mistake in programming allowed the worm to spread more widely than originally intended.[41]

In the realm of technological evolution, advancements in cyberspace stand nearly at the top of the evolutionary food chain. The pace of change, however, is not the only unique aspect of cyberspace that induces anxiety. Rather, a set of intrinsic characteristics all combine to produce an environment that is conducive to increased panic. In particular, the rapidly growing ubiquity of cyberspace, combined with its speed and potential for anonymity, create an environment in which the adversary's intent is increasingly opaque and the targeting of civilians is increasingly feared.

Ubiquity. Cyberspace is everywhere. From electronic banking to the global positioning system, cyberspace touches many aspects of modern life. Today's generation of teenagers may never step in to a brick-and-mortar bank or know the pleasures of poring over a map to route-plan for the family vacation. Nor must one directly seek out connectivity; the internet will likely find him. Even one who eschews the connectivity of the modern world will still likely eat produce that was planted with the aid of satellite imaging and remotely managed farming implements or make a phone call that is at some point routed across digital trunks. As cyberspace touches more aspects of everyday life,

[40] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Threat Level* (2011), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[41] Noah Shachtman, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals," *Wired* (2012), http://www.wired.com/dangerroom/2012/07/ff_kaspersky/all/.

society is presumed to become more dependent upon it and, as such, anxiety over its loss rises. The hyper-connectivity of cyberspace is no surprise; indeed, connections are what enable cyberspace to exist in the first place.

The Age of Information grew largely uncontrolled, the desire to connect often crowding out any peripheral view of associated risks. As such, today's economic, sociological, and security architectures have become increasingly reliant on frameworks built, in many cases, without much conscious concern with regard to its fragility. Even in the military sphere, where security is ostensibly a primary concern, many deficiencies and vulnerabilities exist. Increased interaction and connectivity necessarily expose systems to greater risk. Furthermore, this ubiquity lends itself to a deterministic view of its impact. It is tempting to envision this omnipresent technology propelling itself forward along a path of advancement because "the thingness or tangibility of mechanical devices…helps to create a sense of causal efficacy made visible."[42] While such outlooks are overly deterministic, fear is strongest where a modicum of truth is present. The paranoia surrounding the rise of cyberspace is no exception. Technology does, after all, exhibit a certain momentum of its own: technology helps shape the society that shapes it back.[43] As technology and society interact and the two become more interdependent, the thought of holes in the proverbial firewall is unnerving. Cyberspace's ubiquity makes it hard to secure, even for the world's most dominant militaries. Furthermore, even if the military could easily establish control in cyberspace, the speed at which transactions occur would likely still induce unease.

Speed. At the dawn of the twentieth century, operations through the air domain began to chip away at the tyranny of distance. By the end of the century, it had been obliterated. Airplanes may have broken the speed of sound, but operations in cyberspace were moving at the speed of light. According to Betz and Stevens, "[r]eduction of time and space into instantaneous connection increases the number of actors that may be affected by forms of power that were previously constrained by physical and temporal

[42] Merritt Roe Smith and Leo Marx, *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994), xi.
[43] Smith and Marx, *Does Technology Drive History?*, 101-13. For more on the concept of technological momentum, refer to T.P. Hughes's excellent chapter describing his attempt to find a middle ground between the extremes of technological determinism and social constructivism.

separation."[44] In cyberspace, targeting a system half a world away may require months or even years of intelligence preparation to understand the networks and connectivity, but executing an attack may require less than a second. The introduction of cyberspace speeds everything up, even outside the confines of the electromagnetic spectrum. The ability to move data nearly instantaneously across physical and, perhaps more importantly, political boundaries, fundamentally alters operational calculus.[45] Information that was once constrained to the dominion of the intelligence analyst is now directly integrated into weapon systems. Pushing information forward to the trigger-puller in an effort to improve battlefield awareness has become the norm. As data continues to seep its way into all aspects of conflict, speed and the ability to act before the adversary increasingly become "the coin of the realm."[46] This leads to the next critical aspect of cyberspace: the potential for anonymity.

Anonymity. One of the most vexing problems of cyberspace is the extreme difficulty associated with identifying who, exactly, is doing what. Cyberspace introduces a unique element of uncertainty unparalleled in the physical domains. Granted, some advocate for the promise of "context" to help resolve the attribution problem. Some assert that "the strategic context would reveal a great deal about the attacker,"[47] but Susan Brenner, a respected cyber scholar, counters that "cyberspace can fracture the crime scene into shards and make it much more difficult to determine the ultimate point of origin of attack."[48] She proceeds to take the reader through a mind-tangling scenario of "what-ifs," that, at one point, has Chinese nationals attempting to frame Pakistan as the source of an attack ostensibly designed to frame China.[49] While this is an admittedly unlikely scenario, it is illustrative of the possible permutations of attribution involved in a

[44] Betz and Stevens, *Cyberspace and the State*, 39.
[45] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 255-56.
[46] J. Brenner, *America the Vulnerable*, 199.
[47] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 319.
[48] Brenner, *Cyberthreats: The Emerging Fault Lines*, 150.
[49] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 140.

medium where there is little concrete and attributable evidence of origin.[50] It is probably unrealistic to expect nations to make critical national security decisions based largely on circumstantial evidence. Moreover, even in cases where locational attribution is possible, it is often a challenge to assign ultimate responsibility or do so officially.[51] Furthermore, anonymity often makes it difficult to discern what the enemy aims to achieve.

Opacity of Intent. Determining intent is a challenge in any medium. Even the best social engineer can detect emotion but not *why* the emotion is displayed.[52] The problem is even more vexing in cyberspace, where there is no face to read, no gun to see, and no physical movements to observe. The environment is difficult to conceptualize and those operating in it can easily disguise their appearance and mask the true aim behind their actions. This can be a significant problem for decision-makers. It results, for instance, in a definitional ambiguity that prevents clear delineation between attack and espionage.[53] Worse yet, the speed of operations within the cyber domain creates an environment where intentions can change, and more importantly, be acted on, in the blink of an eye.[54] From a strictly technical perspective, it is nearly impossible to derive intent from action. "A foreign penetration designed merely to gather intelligence and one to preposition a cyberattack weapon" often look the same.[55] In cyberspace, it is hard to tell where the enemy is aiming, which may be the most unnerving prospect of all. The

[50] Derek S. Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 10.

[51] Joel Brenner provides an excellent example of this quandary in his account of "Operation Aurora," a series of 2010 attacks against a bevy of companies throughout the United States and Europe wherein China systematically broke into thousands of systems and absconded with not only personal data, but trade secrets. Early that year, acting on information gathered by one of the primary victims, Google, the US State Department spokesman announced that the United States would issue a formal démarche to the Chinese government on the issue "in the coming days." As days turned into weeks, the case was strengthened through further investigation and reporting. By mid-May, the State Department had nearly unassailable proof of Chinese government involvement through human sources. No démarche ever came. Meanwhile, the Chinese became publicly indignant and accused the United States of attempting to "preserve its hegemonic domination" under the guise of promoting free speech and a free Internet. While a number of factors may have contributed to US reluctance to publicly condemn the Chinese government, the difficulty and uncertainty of attribution must have played a significant role, at least early on. Even after solid information was ascertained from human intelligence, the United States could not take it to the government without fear of divulging its sources. See J. Brenner, *America the Vulnerable*, 45-51.

[52] Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (Indianapolis, IN: Wiley, 2011), 129.

[53] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 82.

[54] J. Brenner, *America the Vulnerable*, 156.

[55] J. Brenner, *America the Vulnerable*, 215.

unique combination of ubiquity, speed, anonymity, and opacity of intent have led to an undercurrent of anxiety over the perception that civilians are today more vulnerable than ever before.

Civilian Vulnerability. According to a number of popular books and newspapers, especially in developed states, threats in cyberspace represent a clear and present danger. Critical national infrastructure, national economies, and property (both physical and virtual) are all put at risk by the prospect of warfare in cyberspace.[56] For Americans, the prospect of effects on the homeland is even more unnerving. The scenarios most often described are played as home games–not something the United States is familiar or comfortable with. Not since the Civil War has there been a true war on American soil, excepting the so-called War on Terror, undertaken as a result of the terrorist attacks of 11 September 2001.[57] Americans, quite understandably, prefer it that way. Technology, however, just as it did with the advent of flight, has, in the case of cyberspace, eliminated pure geography as a guarantee of sovereignty and safety. There is no ocean in cyberspace to separate the United States from her enemies; they are but a click away.

Susan Brenner predicts that whereas "[r]eal-world warfare is overt and destructive…cyberwarfare will be subtle and erosive….In the real, physical world, warfare is like professional football: only the designated players participate. In the cyberworld, warfare will be much more catholic: civilians are likely to be prime players and prime targets."[58] Furthermore, the ambiguity of both source and intent enhances the complexity of determining response. In the physical world, the line of demarcation can generally be drawn at the physical borders of the state. Internal threats are the responsibility of civilian law enforcement while external threats are the province of militaries.[59] Law enforcement combats crime while armies fight wars. In cyberspace, however, the line of demarcation is not often clear and therefore, lines of responsibility are blurred. Though civilians are caught up in warfare, the world has developed a set of

[56] Betz and Stevens, *Cyberspace and the State*, 11.
[57] President George W. Bush used the term "war on terror" in a joint session of Congress on 20 September 2001. George W. Bush, President, United States of America (address before a joint session of the congress on the United States response to the terrorist attacks of September 11, Washington, DC, 20 September 2001).
[58] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 10.
[59] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 79.

rules regarding “noncombatants” and how they may be treated. Civilian casualties are, in war, normally a byproduct of purely military action. In cyberspace, however, Brenner worries there may be no room for noncombatants, as such. As civilians become more vulnerable to attack, she opines, nations target them.[60] Furthermore, the persistence of the “internal-external threat dichotomy” inhibits the systemic ability of civilian law enforcement and military personnel to join forces in order to combat ambiguous cyber threats, which undermines efficient response and introduces further uncertainty along with an attendant anxiety over how to react.[61]

Right Time, Right Space

The time is ripe for panic in cyberspace. The current geopolitical landscape, combined with the ubiquity, speed, and anonymity of cyberspace, not to mention its rapid rate of growth, creates an environment conducive to nurturing seeds of anxiety and surrender to determinism. The international environment is fluid and the West is anxious about the prospect of a multi-polar future. The United States in particular has of late tended to seek the comfort of analogies that, if perhaps ultimately more precarious, were less strategically ambiguous. Cyberspace began its meteoric rise as the Soviet Union was completing its fall. Following a brief period of relative stability underpinned by nearly unparalleled US hegemony, the world began once again to contemplate an uncertain future. This “Age of the Unthinkable” reflects a “new world disorder” within which the uncertainties of cyberspace are magnified.[62] Cyberspace is to the twenty-first century as nuclear weapons were to the dawn of the Cold War and, before that, as aircraft were to the world wars. Each period of international upheaval served to magnify and amplify the anxiety associated with the introduction of groundbreaking new technology. As the geopolitical environment shifted, mankind struggled to bend each new technology to the service of its political ends. The unique aspects of cyberspace exacerbate today’s uncertainty.

Simply put, strategic calculations in the context of cyberspace are tough. How does a state respond to cyber operations? What constitutes an attack and what is merely espionage? A state could take a page out of the Bush Doctrine playbook and simply

[60] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 10.
[61] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 98.
[62] Betz and Stevens, *Cyberspace and the State*, 128.

declare that nations are responsible for all aggression (assuming, for a moment, the operations can even be called aggression) emanating from inside their borders, but that too is problematic, considering that if hacking for sport and crime are included under the umbrella, the United States leads the way. The United States may not wish to set a precedent of national responsibility in the ambiguous realm of cyberspace, especially considering the ease with which operations can be conducted virtually from nearly anywhere on the globe.[63]

"We use the term *cyberattack* to include everything from network nuisances to systematic espionage to disabling electronic sabotage….The war/not war question has also become more difficult – and less useful – because the line between war preparation and war fighting has become blurred….Determining when an attack amounts to war is important, but it won't enlighten us about the nature and urgency of the threat or how to deal with it."[64] Much like the space race during the Cold War, the combination of a growing reliance on ever-more scientific warfare and an ambiguous strategic environment, the separation between military and civilian activities is growing increasingly hazy.[65] "The age of perpetual technological revolution and total Cold War was inevitably the age of politician of the military and the replacement of intuition, honor, and battlefield courage by the exploits of the machine. In such an age, what training or virtue made the soldier more qualified to judge matters of national defense?"[66]

These sorts of conversations make people uncomfortable. When gazing at an uncertain future while grappling with technological growth accelerating at a nearly inconceivable pace, it is little wonder that many seek the warm embrace of determinism. Inevitability, after all, liberates one from the shackles of responsibility. Instead of seeking to define the prospects of an alternate future, one can remain content to shout from the hilltops the dangers of the coming storm, lambasting those who are blind to its approach. If only everyone would shore up the defenses and fix bayonets, the country might be saved. Hyperbole aside, one must acknowledge that vulnerabilities *do* exist. Be that as it may, it seems that many of the warnings conflate vulnerability and threat. This

[63] J. Brenner, *America the Vulnerable*, 51.
[64] J. Brenner, *America the Vulnerable*, 155.
[65] Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore, MD: Johns Hopkins University Press, 1997), 174.
[66] McDougall, *The Heavens and the Earth*, 214.

is not to say there is not threat, merely that determination of threat requires an additional level of analysis. Vulnerability must be matched with adversary capability and, most importantly, intent.

Risk does not equal likelihood. Furthermore, and perhaps most dangerously, the tenor of the today's cyberspace conversations establish a foundational understanding of cyberspace which, through their deterministic interpretation of the future of conflict, skirt the edge of redefining the very nature of war itself. In attempting to establish the revolutionary impact of operations by, with, and through cyberspace, those who would warn of the coming dangers may have committed strategic overreach. While the dystopian future they predict is certainly a possibility, it is not as inevitable as some foresee.

Prospects for a Sunnier Future

Since the beginning of time, man has grasped for an edge in the struggle for survival. Gunpowder, machine guns, airplanes, and countless other technologies were all heralded as revolutionary inventions, certain to change the face of warfare. Further, many of these technologies spurred debate over whether the very nature of warfare had been fundamentally altered. Each new technology seemed to transform the landscape to such an extent that, at least to some, war would never be the same. Such is the case in cyberspace. Much like air power in the early twentieth century, operations in cyberspace offer a new context within which to consider the nature and character of war. Given the comparatively fledgling nature of the domain and intrinsic rapidity with which it expands, contemplating its role in future conflict becomes increasingly important, especially as it proliferates ever deeper into both civil and military systems. While cyber power advocates have begun the early stages of analysis regarding its impact, they have barely scratched the surface. Furthermore, the body of work appears to reflect an undercurrent of anxiety bordering on panic regarding what is judged to be a public and bureaucratic indifference to the threat posed by the continued proliferation of vulnerabilities.

A significant amount of contemporary literature focuses on risk to the detriment of a balanced discussion regarding the broader aspects of cyber operations. A truly worthwhile investigation of cyberspace necessitates a more objective approach. An accurate appraisal requires understanding of the nature of cyberspace and its impact on the character of conflict. First, much of the rhetoric tends to lump all cyberspace effects together under an implied heading of destruction. Establishment of a more precise lexicon with which to describe the effects of cyber operations reveals that at least some of the panic may be more hype than reality. Next, war itself must be examined in an effort to bound the influence of cyberspace and understand its limitations vis-à-vis war's fundamental nature. Closer examination enables construction of a more balanced view of cyberspace that recognizes its potential for radical changes to war's character while maintaining a healthy respect for the underlying continuity of its nature. Additionally, it allows further investigation of another often-overlooked unique aspect of cyber operations, enhanced precision, and what effect this characteristic might have on the future of conflict in cyberspace. Finally, having established a nuanced perspective of cyberspace in the context of war, one can more accurately evaluate the prospects for norm-based constraint in the international cyberspace arena. Though there remains no guarantee a primrose path of peace and cooperation through cyberspace, more in depth analysis does point toward the possibility of a less dystopian future, one that should be considered lest the world mistakenly prepare for a future that never comes or, worse yet, inadvertently usher in a darker tomorrow. Put simply, the future of cyberspace is not preordained.

Clarity Through Categorization

Uncertainty permeates contemplation of cyber conflict. From difficulties of attribution to scope of collateral damage, to potential effect on the intended target, conflict in a world of ones and zeroes is necessarily opaque.[67] This often leads to a lack of precision regarding discussions of effects, which in turn leads to excessive predictions and increased anxiety. In order to better delineate and ascertain the likelihood of effects in cyberspace it is first necessary to establish a more precise rubric with which to classify cyber effects on society's ability to function and maintain internal order.[68] Effects in

[67] Reveron, "An Introduction to National Security and Cyberspace," 10.

[68] This rubric is based on a construct described by Susan Brenner in her book, *Cyberthreats: The Emerging Fault Lines of the Nation State.* Susan Brenner posits a parallel schema in her examination of potential effects of cyberterrorism on societies. The schema used here is broadly based on her classification system, but applied more generally to *actors* in cyberspace rather than just terrorists. Brenner, *Cyberthreats: The Emerging Fault Lines*, 43-50.

cyberspace can be more appropriately described in terms of *distraction*, *disruption*, and *destruction*.

Distraction. In the context of cyber effects, distraction refers to the use of cyberspace primarily in pursuit of psychological effects.[69] Damage to banking systems, for instance, threatened but not even necessarily carried out, may lead to mass withdrawals and an erosion in confidence and subsequently the market. A more insidious scenario might involve an adversary hacking into a supposedly secure government computer system in order to send a bogus message regarding a weapon of mass destruction placed in a metropolitan center and set to go off in the very near future. Trading on the inferred credibility of such a message, such a threat could very likely lead to immediate evacuation followed by gridlock, which would in turn drive panic. Roads would be clogged, mass transit would be overrun, and hysteria would likely ensue. It would not be a stretch to envision a rapid breakdown of society, albeit admittedly localized to the affected city.[70] Though destruction could conceivably result in the second scenario, it would not reach the level of *societal* disruption. Martin Libicki, a senior management scientist at the RAND Corporation, asserts that most cyber effects over the last 20 years fall into this category. Despite two decades of dire predictions, no cyber attack has ever resulted in loss of life and very little physical destruction has occurred.[71] Many predictions of cyber Armageddon probably fit best in this category.

Disruption. Stepping up the impact scale, *disruption* refers to actions whose results "undermine a civilian populace's faith in the stability and reliability of essential infrastructure components such as mass transit, power supplies, communications, financial institutions, and health care services."[72] The key difference between distraction and disruption is that with distraction, the perpetrator merely induced the population to "*believe* a system had been compromised," whereas with disruption, systemic damage is the goal.[73] Disruption seeks to affect the underlying foundation of some aspect required for a society to function efficiently. Actual interference with a nation's power grid, for

[69] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 47.
[70] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 46-47.
[71] Martin C Libicki, "Cyber Operations Can Supplement a War, but They Cannot Be the War," *The Rand Blog* (2012), http://www.rand.org/blog/2012/12/cyber-operations-can-supplement-a-war-but-they-cannot.html.
[72] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 47.
[73] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 48.

instance, would fall into this category, as would an attack on a major transportation sector such as the air traffic control system. The aim of disruption, more than a specific *object*, is the bonds and connections that allow the systems to function.[74] There is no need to blow up 100 airplanes if they can be prevented from taking off in the first place. Wreaking havoc, in this case, does not necessarily entail physical destruction.

Destruction. The final category, *destruction*, is the most frightening, yet also, at least so far, least likely. Here, in this category, is where the most feared effects lie: no deaths have yet been attributed to a cyber attack, but were they to, they would most likely fall within this category. *Stuxnet*, the attack on Iranian centrifuges, is an example of destruction via cyberspace, albeit one targeting a capability as opposed to a person.[75] Damage to hydroelectric dams or to generators connected to a national power grid would also fall into this category, and are examples of attacks that might one day result in fatalities. Destruction in the physical world is enabled through the increasingly electronic control of major infrastructure systems. Susan Brenner discounts the characterization of most attacks that might fall into this category as "cyberattacks," arguing that though computers are used to *trigger* them, they are more appropriately referred to as *nuclear* catastrophes, for instance, in the case of the targeting of the nuclear power plant, rather than *computer* catastrophes.[76] Her argument, however, is disingenuous and does a disservice to discourse regarding this most feared of cyberspace attack vectors. Though in these cases cyberspace is admittedly a means rather than an end, it is undeniably central to the effect. Without cyberspace, and operations within it, these effects generally require close, physical access and often some other means of damage such as a bomb or at the very least some physical form of destruction. Cyberspace and control of these systems via computer are the precise avenues of attack without which, the attack may be so difficult as to be considered impossible for all intents and purposes.

Much of Fear is Fear Itself. In an effort to shine a spotlight on the possible, many often trumpet the horn of Armageddon and in so doing, conflate the effects of distraction, disruption, and destruction. With a more nuanced rubric in hand, it becomes

[74] Robert J. Bunker, "Weapons of Mass Disruption and Terrorism," *Terrorism and Political Violence* 12, no. 1 (2000): 37.

[75] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," *ISIS* 15 (2011): 1.

[76] S. Brenner, *Cyberthreats: The Emerging Fault Lines*, 45.

clear that the effects predicted often fall short of the Armageddon so routinely presaged. The attacks on Estonia and Georgia, for instance, two oft-referenced cases of cyber warfare, generally fall into the low end of the distraction category. In 2007, in what was widely referred to as the "first cyber war," Estonian governmental and financial institutions were targeted with a massive distributed denial-of-service attack following a governmental decision to move a Soviet war memorial.[77] There were reports of "crippled…communications infrastructure,"[78] but upon "closer examination, the evidence in support of these claims is rather equivocal."[79] Online banking was shut down for a total of three and a half hours over the course of two days and the Estonian parliament's email system was disrupted for several days, but there was no permanent damage, no loss of life or territory, and no major disruption of essential services.[80] Though Estonia did petition for NATO intervention,[81] fear of pending physical measures by the Russians may have played a larger role than the cyber attacks themselves. Similarly, there appears to have been "far more smoke than actual fire" surrounding the much ballyhooed Russia versus Georgia cyber attacks in 2008.[82] In both cases, Russian security services are widely thought to have contributed to planning if not prosecution of the operations.[83] Of course, one might argue that the Russians were simply exhibiting restraint, holding back true capabilities so as not to tip their own hand. A simpler explanation, however, might be that the Russians simply gave it their best cyber shot and "that was it." [84] In any case, the damage in both cases was minimal and probably best fits into the "distraction" category.

Even in the case of *Stuxnet*, considered by many to be the first publicly acknowledged deployment of a state-developed cyber weapon, the damage was extraordinarily minimal and contained to a specific piece of equipment in a single

[77] J. Brenner, *America the Vulnerable*, 127-30.

[78] Richard B. Andres, "Strategic Cyber Offense, Cyber Defense, and Cyber Deterence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 99.

[79] Betz and Stevens, *Cyberspace and the State*, 31.

[80] Betz and Stevens, *Cyberspace and the State*, 31.

[81] Andres, "Strategic Cyber Offense, Cyber Defense, and Cyber Deterence," 99.

[82] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 36.

[83] Betz and Stevens, *Cyberspace and the State*, 61.

[84] Betz and Stevens, *Cyberspace and the State*, 31.

facility.[85] *Stuxnet* employed the use of physical destruction, which might at first glance place it in the "destruction" category. More germane to the discussion at hand, however, is the end result, the actual *effect* of the destruction: not the major and widespread catastrophe envisioned by the typical destruction scenario but merely disruption of the Iranian nuclear program. None of this is to say that more serious attacks are not possible, but it is telling that three of the major examples of cyber attacks in the last decade, when examined more closely with a dispassionate eye, fall far short of the pandemonium envisioned. Clearly, "cyberspace alters much but it does not change everything and it changes things in the military sphere, which has traditionally preoccupied strategists, considerably less than has been supposed."[86] Indeed a closer examination of the impact of cyberspace on war reveals that while it may have significant impact on war's character, its ability to alter war's nature is highly doubtful and as such, constraint, even in the realm of cyberspace remains a possibility.

The Eternally Uncertain Nature of Warfare

Mankind has always yearned to eliminate uncertainty in war and the thought that machines might somehow mitigate the fog and friction of war is supremely appealing.[87] As machines gain in intelligence, they drive a tendency to underestimate the chaos and uncertainty of war.[88] Machines, after all, are unemotional and supremely rational. Theoretically, the more prominent their place in warfare, the less irrational and unpredictable it will be. Some see the Age of Information as the dawn of a new era, one in which the unpleasant confusion of conflict is minimized and eventually eradicated. This view of the promise of cyberspace is, however, a reflection of the propensity to conflate information with knowledge and understanding. The chimera of perfect knowledge is no more obtainable today than it was before man began to harness the electromagnetic spectrum. The intelligent enemy deceives today as he did 1,000 years ago. His morale cannot be discreetly measured via network traffic. His intent remains opaque, even to the unblinking eye of a surveillance satellite. While the forces of

[85] Betz and Stevens, *Cyberspace and the State*, 27.
[86] Betz and Stevens, *Cyberspace and the State*, 12.
[87] Antoine J. Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, Critical War Studies (New York: Columbia University Press, 2009), 9.
[88] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004), 49-52.

uncertainty and friction can be reduced, the fact that "war is an interaction between intelligent foes," means they will never be eliminated.[89]

In spite of significant efforts to loosen its hold, chaos maintains a firm grip on war. It permeates operations at all levels. Accurate and timely information, while necessary, is not sufficient for victory. Clausewitz's military genius will always be required to combat an ever-present level of uncertainty.[90] The successful strategist is he who matches "a changing and expanding universe of mental concepts" most closely "to a changing and expanding universe of observed reality."[91] Cyberspace offers leaders a host of tools with which to prosecute war, but they "are exactly that – *tools*, useful in some situations, useless in others."[92]

Exploitation of cyberspace remains critical to many aspects of modern warfare, but does not guarantee victory. Wars are fought to achieve some end. Indeed, this end, or rationale, is what separates war from mindless murder and violence.[93] Policy remains the impetus of warfare. No technology, not even cyberspace, can change this. Despite mankind's greatest attempts, control over warfare remains elusive, for mankind remains involved in its prosecution. As long one nation struggles to impose its will on another, political ends will define war. "The information age may create new motivations for the resort to war, but it will not produce wars that are not the continuation of policy."[94] Human involvement dictates that in war, uncertainty and friction will dominate the pursuit of political objectives. Cyberspace may alter the character of war, but its nature remains fixed. Furthermore, contemporary prognostication regarding the future of war by, with, and through cyberspace often misses this point. While cyberspace may offer increased and varied ways to affect an adversary, its mere existence does not compel to action. War remains set in a broader geopolitical context, one which affects state action no matter what tools are at its disposal.

[89] Lonsdale, *The Nature of War in the Information Age*, 54-60.
[90] Carl von Clausewitz, Michael Howard, and Peter Paret, *On War* (Princeton, NJ: Princeton University Press, 1984), 100.
[91] Quoted in John R. Boyd, "Destruction and Creation," in Bousquet, *The Scientific Way of Warfare*, 190-91.
[92] Sanger, *Confront and Conceal*, 243.
[93] Lonsdale, *The Nature of War in the Information Age*, 28.
[94] Lonsdale, *The Nature of War in the Information Age*, 28.

Politics Still Matter

Often forgotten in dramatic predictions of war in cyberspace is the context within which it would be executed. Discussions of so-called cyberwar seem to imagine a primarily one-way relationship in which the digital world can directly affect the physical, but appears to remain largely free from the political constraints that govern interaction in the physical realm. Operations in cyberspace, though, as with all interaction on the international stage, nest within a larger, pre-existing context. They do not play out on a pristine and independent field. Indeed, Joseph Nye and Robert Keohane, two renowned scholars of international relations, asserted that "information does not flow in a vacuum but in a political space that is already occupied."[95] Politics still matter, even in the virtual world of cyberspace.

"The issue, therefore, is not cyberwar, but cyber *in* war."[96] The nature of war is unchanged; even smart phones and robot planes cannot alter the bond between policy and war. To assume that war within cyberspace will independently progress toward indiscriminate Armageddon is to deny Clausewitz's fundamental dictum that war (even war in cyberspace) is an extension of politics.[97] Cyber power, therefore, must be subservient to policy, which undermines the determinist vision of unimpeded escalation of conflict in cyberspace. As with all forms of warfare, restraint in cyberspace may occur for a number of reasons ranging from limited policy objectives, to proportionality, to fear of retribution.[98] Furthermore, unbridled escalation may prove strategically disadvantageous. As alluded to above, cyber power has yet to prove any coercive ability.[99] Estonia ultimately moved the Bronze Soldier of Tallinn, Georgia withstood its own cyber attacks, and today Iran continues to pursue its nuclear program. Granted, cyber operations likely played some part in the strategic calculus of each case, but their effects appear to have been a far cry from the dramatic tales spun by cyber

[95] Quoted in Morozov, *The Net Delusion*, 25.
[96] John B. Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 209.
[97] Clausewitz, Howard, and Paret, *On War*, 87.
[98] Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," 209.
[99] Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," 215.

prognosticators.[100] Many who continually warn of impending doom make the same error as some early air power theorists. They are blinded by the perceived power of this new domain of warfighting. In reality, cyber power, as with air power, sea power, space power, and ground power, is merely one portion of the overall strategic environment.

Cyberspace does not alter the nature of the international system. In the end, the cause of war derives from a number of variables, each specific to time, space and the relationship between two states. The determinist view that assumes conflict in cyberspace will escalate simply because the capability exists belies a fundamental misunderstanding of this notion. The sudden introduction of technology, revolutionary though it may be, does not suddenly cause the international community to throw out strategic calculus and undertake operations simply because it can. Society has dealt with change before. The telephone baffled the average citizen of the 1870s, but it was ultimately assimilated to the existing paradigm.[101] It may have revolutionized means of communication, but did not change their ends. Such is the case with cyber power. Cyberspace did not and cannot alter the nature of war, no matter how vulnerable its ubiquity might make one feel. Would that it could; perhaps it would increase the prospects for peace. Vulnerability is not a guarantor of strategic success. Though conflict by, with, and through cyberspace may have the ability to inflict significant disruption, it "does not work outside the dialectical nature of strategy, in which the enemy's actions and his robustness will usually deny a strategic campaign the strategic success it desires…"[102] In his seminal study of mankind's history in space, Walter McDougall notes that "the Space Age would neither abolish nor magnify human conflict, but only extend politics-as-usual to the new realm."[103] Such is the case in cyberspace. War will carry on as an extension of politics and be forever dominated by uncertainty if for as long as it is an interaction between intelligent foes.[104]

Operations in cyberspace have not altered the nature of war, nor do they threaten to in the near future. The histories of similarly groundbreaking weapons of the past may

[100] Again, it is important to note that the argument here is not that cyber effects could not play a larger role in the future. Rather, these examples are intended to reflect the possibility of a future in which cyberspace effects to not redefine the geopolitical environment but instead are integrated into it.
[101] Betz and Stevens, *Cyberspace and the State*, 12.
[102] Lonsdale, *The Nature of War in the Information Age*, 170.
[103] McDougall, *The Heavens and the Earth*, 414.
[104] Lonsdale, *The Nature of War in the Information Age*, 60.

illuminate an alternate future, one less defined by unrestrained conflict and more realistically reflective of the role of constraint in strategic calculations. The introduction of cyberspace, in fact, may have quite the opposite effect on the character of war. Most contemporary literature focuses on the vulnerabilities introduced through cyberspace but fails to examine another, possibly more revolutionary aspect of operations in cyberspace: the potential for unparalleled precision.

Hyper-Precision

One little-explored facet of cyberspace is the potential for what this author terms “hyper-precision.” Though much of the current cyber discussion appears to revolve around the fear of WMD-style destruction, cyber technologies appear to be capable of producing precision effects unparalleled in the annals of modern warfare. Rather than unleashing a tidal wave of indiscriminate warfare, cyberspace may hold the keys to *decreased* effects on civilians. This is an important consideration, considering the established preference to avoid civilian casualties. Furthermore, the case of *Stuxnet* appears to provide empirical evidence suggesting that exploitation of cyberspace’s hyper-precise nature may ultimately be *more* strategically advantageous than the indiscriminate methods envisioned by many cyber prognosticators.

In Search of Humane Killing. In Operation Desert Storm, when US air power was able to put a bomb down a ventilation shaft, the world sat up and took notice.[105] A new pinnacle of precision had been reached. Suddenly, it appeared, the United States had found a way to deliver violence to an enemy while avoiding many of the moral or political hazards that normally complicate such matters. With so-called smart bombs, the Americans could hit just the Bad Guy. Certainly, mistakes continued to occur, the Bad Guy was not always alone, and civilians were sometimes killed. American precision set a new precedent, though, for discrimination in warfare. This precedent followed a decades-old trend of increasing precision in order to improve discrimination on the battlefield. The argument for cyber Armageddon presupposes logic of capacity as driver of use. It reflects a Pandora’s Box approach to violence and weapons: if you build it, they will use it. As was demonstrated in the previous chapter, however, this has not

[105] Lt Col Roy A. Griggs, "Technology and Strategy," *Airpower Journal* 10, no. 2 (1996), http://www.airpower.au.af.mil/airchronicles/apj/apj96/sum96/griggs.htm.

always been the case. In fact, in the case of two of the most destructive and indiscriminate weapons in the history of mankind, chemical and nuclear arms, Pandora's Box was actually closed again even after it was opened. The world has shown a capacity, indeed, a propensity for restraint, even in times of near-total war.

Whether for moral, institutional, legal, or pragmatic reasons, humanity has exhibited an aversion to civilian casualties. Chapter 2 demonstrated that in the case of some of the most fearsome weapons in history, a desire for discrimination drove constraint. History reflects a general aversion to civilian involvement, direct or indirect, in the horrors of war. With the exception of the French Revolution, the sovereign has almost always directed an army into battle. Whether it was the knights of mediaeval times or the *condottieri* of the Renaissance, a separation existed between civilian and soldier. The very existence of a draft or conscription, instituted by nearly every country at some point in its history, indicates the necessity of inducting men into an organization separate from the general populace. With few exceptions, warfighting has been the exclusive preserve of the warfighter. Many predictions, however, appear to assume that cyberspace will wipe away this separation. By their logic, if civilians can be targeted by, with, or through cyberspace, then they will be. This argument of causality by capacity, though, is fallacious. Were capacity the dependent variable, countries would be dropping bombs simply because they could. Given its dominant position vis-à-vis air power, such logic would predict that the US Air Force would be much less discriminant in its mission execution than it is. If capacity is key, what explains the restraint exhibited in the landmine, chemical/biological, and nuclear arenas? Perhaps, rather than a descent into indiscriminate warfare, cyberspace's potential for precision will strengthen the exclusivity of war as the domain of the warfighter.

The advent of cyber weapons may usher in a shift in the character of warfare toward precision and improved discrimination. Rather than a downward spiral toward increased targeting of civilians, warfare in cyberspace may offer the opportunity to affect an enemy's ability to wage it while shielding his population from the horrors of its violence. To paraphrase the Nye and Keohane quotation from above, operations, even those in cyberspace, occur in a political space that is already occupied.[106] If decimation

[106] Morozov, *The Net Delusion*, 25.

of the enemy's population were the only strategic consideration, then cyber doomsayers might be justified in their predictions of the inevitable escalation of warfare in cyberspace. Fortunately, the enemy's population is not the variable upon which strategic success depends. The prospects for cyberspace, in fact, may point toward a direct correlation between hyper-precision and strategic advantage.

The Strategic Advantage of Hyper-Precision. American joint planning doctrine defines two different operational measurements of success: measures of performance (MOP) and measurements of effectiveness (MOE).[107] In colloquial terms, MOPs ask, "Are we doing stuff right?" and MOEs ask, "Are we doing the right stuff?" Though focused on the operational level of warfare, the separation between MOPs and MOEs point to a larger consideration, one that is especially apropos to discussions of warfare in cyberspace; namely, there is a difference between *combat* effectiveness and strategic *effectiveness.* Measurement of combat effectiveness alone can lead to strategic futility.[108] Insofar as many discussions of warfare in cyberspace focus on the vulnerability of civilian infrastructure and its susceptibility to sabotage, the operational, or combat effectiveness is privileged at the expense of strategic considerations. Coercion through punishment of civilians has rarely been proven military effective in the first place.[109] Furthermore, the potential for a "shock and awe" campaign reminiscent of the US strategy during Operation Iraqi Freedom notwithstanding, the crude and overt approach of targeting civilian infrastructure carries with it a strategic cost of surprise. In operations short of total war, the cost of alerting the adversary may not exceed the benefits gained through infrastructure degradation. Conversely, exploitation of cyberspace's potential for hyper-precision may offer at best a closer approach to Sun Tzu's ideal of victory without bloodshed and at worst, a useful ability to buy time through clandestine operations.[110]

Cyber weapons "work best when the victim doesn't even know he's being robbed."[111] Cyberspace offers strategists the ability to achieve effects with an extraordinary amount of deniability and stealth. Furthermore, the nature of cyberspace

[107] Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011, III-44-III-46.
[108] Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 56-57.
[109] Pape, *Bombing to Win*, 10.
[110] Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 2005), 15.
[111] Quoted in Sanger, *Confront and Conceal*, 191.

allows an improved ability to disguise operations as anything but intentional and directed. According to open-source reporting, *Stuxnet* is a perfect example of this phenomenon of hyper-precision in pursuit of strategic effects. This, in fact, is exactly what the designers of Olympic Games, as the operation was officially known, had in mind.[112] Centrifuge breakdowns would appear to be random accidents and would occur with just enough frequency to prevent final enrichment.[113] In fact, the strategy was brilliant; it was not discovered until a computer security firm (with purported ties to the Russian intelligence) alerted the Iran and the world to the presence of the worm it dubbed "Stuxnet."[114] In theory, had a design flaw not allowed the worm to mistakenly (though harmlessly) propagate worldwide, the Iranians might have eventually been forced to alter their entire enrichment strategy. Surely, Sun Tzu would be proud. Though it fell short of final strategic success, the operation offers insight into another advantage of hyper-precision in cyberspace: its ability to buy time.

In 1948, Western leaders faced a potential crisis when the Soviet Union blockaded the city of Berlin. In search of a middle ground that would not acquiesce but would also minimize potential for escalation, the Berlin Airlift was conceived as a strategy that would buy time to negotiate and bring the crisis to a more amicable end for both sides. Essentially, the airlift bought time.[115] The Berlin Airlift leveraged a unique aspect of air power, namely its ability to bypass the Soviet blockade, in order to mitigate its immediate problem: starving people; and buy time to negotiate a solution to its strategic problem: access to and control of Berlin.[116] Similarly, the exponential improvements in precision available in cyberspace offer avenues to pursue solutions to immediate problems in order to buy time to negotiate solutions to strategic ones. This exponential growth in precision capability offers decision-makers clandestine options to garner breathing space in which to negotiate favorable solutions to vexing strategic problems.

[112] Sanger, *Confront and Conceal*, 188.

[113] Sanger, *Confront and Conceal*, 189.

[114] Shachtman, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals."

[115] Roger G. Miller, *To Save a City: The Berlin Airlift, 1948-1949* (College Station, TX: Texas A&M University Press, 2000), 34, 85.

[116] Miller, *To Save a City*, 34, 85.

With respect to Iran's nuclear weapons program, Olympic Games offered the American administration a hyper-precise method to affect *only* the target of interest. Certainly, other methods of slowing the program were and still are available. However, hyper-precision offered a unique combination of discretion and concealment unmatched by any other capability.[117] A nuclear bomb, for instance, would likely have slowed the program to a much greater extent. However, employment of nuclear weapons is, in addition to indiscriminate, fairly obvious. They necessarily change the strategic positions of all parties relative to each other and the international community, for better or worse. Cyberspace, on the other hand, offers increased potential to maintain the status quo through discrete effects against very specific targets, possibly with no collateral damage whatsoever.

In 1948, the Allies were afraid direct confrontation over Berlin would touch off a war with the Soviets. They opted to take action in order to preserve the status quo and buy time to leverage other capabilities aside from direct military confrontation.[118] Olympic Games offered a similar ability to preserve the status quo. Even better, it offered to do so surreptitiously and discriminately. It offered the American administration a "third choice" to forestall the Iranian nuclear problem and allow more time to not only bring allies more closely into the fold, but to pursue alternative strategies altogether. In the midst of two wars, the prospect of a third (a very real possibility had force been used to delay the program) was inconceivable. "Olympic Games put additional time on the clock…"[119] President George W. Bush, under whom the operation was originally conceived, initially saw his options to deal with Iran as binary: either let the Iranians achieve membership in the nuclear club or go to war to prevent it. Cyberspace delivered an alternative.[120] Furthermore, the results of the failure to contain the spread of the worm actually bolster the case for hyper-precision. As of September 2010, over 100,000 hosts were infected in more than 155 countries, yet only in Iran was any damage produced.[121] The designers of *Stuxnet* were able to produce a weapon that

[117] Sanger, *Confront and Conceal*, 188-93.
[118] Miller, *To Save a City*, 85.
[119] Sanger, *Confront and Conceal*, 207.
[120] Sanger, *Confront and Conceal*, 191.
[121] Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier Version 1.4 (February 2011)* (Symantec Security Response, 2011), 5.

was completely harmless to all but its intended target. Every misfire of *Stuxnet* was guaranteed to be a dud. Though this is not an inherent feature of cyber weapons per se, and bad design could certainly result in inadvertent collateral damage, it is direct evidence of the potential for precision rivaling any weapon in the history of warfare. There is no need to target a city, or even a specific facility, when a microprocessor will do.

Ultimately, Olympic Games mitigated the immediate problem of Iranian near-term nuclear capability and allowed alternate strategic efforts in pursuit of the long-term problem of Iran's nuclear program writ large. Whether Iran eventually gets the bomb is immaterial. The salient point is that operations in cyberspace allowed hyper-precise targeting of Iran's nuclear program in order to slow it down and provide strategic space to negotiate long-term solutions. Cyber operations are, for the current US administration, critical to "a strategy of confrontation and concealment, a precise, directed economy of force."[122] Contrary to mass casualties and targeting of civilians, American decision-makers have discovered the ability of hyper-precision to advance strategic objectives.

If operations in cyberspace are already being undertaken, and it appears that they are, perhaps an international norm is already being established. One of President Obama's national security aides noted that today's technologies enable strategies that mix "precision, economy, and deniability."[123] If cyberspace is strategically more valuable as a tool of hyper-precision than of massive devastation, perhaps there is room for an international norm that will constrain the predicted widespread cyber violence. Perhaps the precedent of restraint set in the arena of landmines, chemical and biological weapons, and nuclear weapons, when combined with the strategically disadvantageous nature of indiscriminate cyber operations, will create an environment in which a norm of restraint will take hold.

Prospects for Restraint in Cyberspace

For every liberal institutionalist prediction, it seems, there is an equally strong realist argument for a future in cyberspace that revolves around power. Indeed, this is generally the case in the physical world; why should it be any different in the world of

[122] Sanger, *Confront and Conceal*, xv.
[123] Quoted in Sanger, *Confront and Conceal*, 246.

cyberspace? That both arguments are valid, though, is exactly the point; an argument for the likelihood of restraint is not unassailable, but neither is the determinist view of unavoidable escalation. Currently, the Obama administration is "allergic" to discussing cyber-offense capabilities out of fear that acknowledgement would "create a pretext for other countries, terrorists, or teenage hackers to justify their own attacks" and though this is a valid concern, the lack of a public stance leaves the world to wonder about the US position on attacks in cyberspace. [124] If the silence persists, the United States may be inadvertently encouraging escalation in cyberspace and is, at the very least, missing an opportunity to lay a foundation for a more structured regime focused on restraint. There are, however, murmurs of indication that the United States understands the opportunity to be grasped in this arena.

International institutions are advantageous to states across the power spectrum. In the case of a hegemon, they provide a vehicle through which to lock in certain strategic advantages with the expectation that their monopoly on power will likely not last for eternity. A stronger state trades some of its power in the present for some stable share in an uncertain future. Weaker states, on the other hand, are incentivized by the prospect of restraint on the part of the stronger powers and increased stability in the geostrategic environment.[125] International regimes provide a normative foundation on which a mutually advantageous stability can be constructed. They allow interstate cooperation in the name of self-interest.[126] Recent statements by US Department of State Legal Advisor Harold Koh indicate that the United States may see value such a regime in cyberspace. According to Koh, "To the extent that we have articulated principles, we have made it clear that we think that the laws of armed conflict in fact apply to cyber operations in war and we have to do a translation exercise of how they apply…but this translation exercise is really at a nascent stage."[127] Could this be the beginning of a US effort to establish norms in cyberspace? The United States has resisted outright arms control in cyberspace, but has signed on to efforts to curb cyber crime, to include signing a global treaty. At

[124] Sanger, *Confront and Conceal*, 265.
[125] G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars* (Princeton, NJ: Princeton University Press, 2001), 55-57.
[126] Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 2005), 43.
[127] Quoted in Sanger, *Confront and Conceal*, 267.

least one author speculates that US resistance stems from the fact that it holds a commanding lead in the arms race there. If that is the case, perhaps Koh's recent statements reflect a desire to lock in some of those advantages for the foreseeable future.[128]

Outside of the United States, international organizations such as the UN and NATO have begun to consider the ramifications of cyber security and possibilities for future international regimes, an encouraging parallel to the beginnings of other regimes, as discussed in chapter 2. NATO's Cyber Center of Excellence in Estonia may offer an especially fruitful location which to explore the prospects for international cooperation and normative behavior. The UN, for its part, has recognized a need for communication on the matter and has begun to explore the role of governance in cyberspace as well as cyber warfare and its impact on international security.[129] Ambassador Henning Wegener, a retired German diplomat and Chairman of the World Federation of Scientists' Permanent Monitoring Panel on Information Security, suggests that since 2001 his own organization has advocated for the UN to take a direct leadership role and furthermore suggests that efforts within the World Summit on the Information Society have actually begun to establish an actual regime through the auspices of the International Telecommunications Union.[130] Two authors have gone so far as to suggest that a Westphalia-style border system in cyberspace is not only feasible, but already beginning to appear.[131] If true, this would provide the strongest indication yet that an international regime is not only plausible, but already beginning to be formed.

A number of authors have suggested looking to space in search of models and lessons that might be applied to cyberspace. Admittedly, the space regime is a work in progress, especially with regard to delineation of legal requirements in peace versus wartime and clear definitions and frameworks regarding weaponization, but these challenges in and of themselves are instructive to nascent cyberspace regime-building

[128] Sanger, *Confront and Conceal*, 265-66, 454.

[129] Rex Hughes, "Towards a Global Regime for Cyber Warfare," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers (Ios PressInc, 2009).

[130] Henning Wegener, "Harnessing the Perils in Cyberspace: Who Is in Charge?" (paper presented at the Disarmament Forum, 2007), 48-49.

[131]Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (2011): 40-44.

efforts.[132] The two domains clearly have significant parallels. One author described two primary challenges associated with the dawning of the space age: “how to contain expensive arms races despite bitter competition and distrust, and how to manage the use of nonterritorial regions like the sea, air, Antarctica, or outer space, within the system of sovereign, territorial states? The answers to both seemed to lie in treaties – for arms control and international law to fill the legal vacuum in outer space – and neither was really new.”[133] In the murky world of space and cyberspace activities, where monitoring of compliance can be challenging, “perceived commitment [is] more important…than results….[t]he very nature of international law is that it is consensual.”[134] By no means does the space regime provide a template upon which to build for cyberspace. It does, however, provide a body of argument and discussion of very similar challenges.

A desire exists on the part of the international community to learn from past challenges and begin to establish a norm of restraint in cyberspace. Whether or not the efforts will ultimately prove successful, the door to regime creation has clearly been opened. Though institutions and treaties are not truly enforceable by any extra-governmental body, they create a normative environment that makes breaking them something less than pain-free. In any case, more time is likely to be necessary in order to discern, and ultimately attempt to shape, any sort of international regime. “The ‘postitivist school’ of space law…argued that law emerged from patterns of common usage – and that could not be invented in advance of knowledge of the facts and emerging national interest. The difficulty in separating military and civilian activities rendered prohibition of the latter all but impossible, and space law in any case would always be a function, not a determinant, of international politics…the patterns of usage of space must be allowed to establish themselves before codification.”[135] Such is the case in cyberspace as well. The cart must not come before the horse, but at least there are indications that they both exist.

[132] Scott James Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27, no. 1 (2009), http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7/.
[133] McDougall, *The Heavens and the Earth*, 177.
[134] McDougall, *The Heavens and the Earth*, 179.
[135] McDougall, *The Heavens and the Earth*, 188.

Conclusion

When it comes to predictions regarding the future of cyberspace, the proverbial glass of international conflict is widely perceived as half-empty. The marketplace for cyberspace pontification is flooded with doomsayers. Strategists have begun to try to provide alternate, or at least more balanced, analyses, but they have been largely stymied by the immaturity of the field and the rapidity of its growth. “Toward” is a common preposition in the titles of such works, as in “Toward a Strategy for Cyber-Power,”[1] “Toward a Theory of Cyber Power,”[2] and perhaps the least auspicious, “Toward a *Preliminary* Theory of Cyberpower”[3] (emphasis added). Titles such as these reflect the challenge of attempting to apply structure to a complex problem with an ambiguous future. A senior U.S. Cyber Command official recently intoned that in the realm of operational planning, there are “a bunch of folks that understand operations and a bunch that understand cyberspace, but very few who ‘get’ both.”[4] Even those directly charged with conceiving of national strategy in cyberspace admit to the inherent challenge of bridging both worlds. Be that as it may, such efforts are crucial in order to gain a clear-eyed view of what, to this point, has been largely painted with a brush of doom and destruction. Experiences of the twentieth century offer an intriguing glimpse at what might be an alternative to that picture.

Signposts Along an Alternate Path

Cybersecurity specialists admittedly face a constant struggle to combat the perplexity and incredulity that often characterize reactions to their attempts to sound an alarm.[5] Perhaps a bit of hyperbole can be forgiven in the service of convincing skeptics of real risks. Embellishment aside, however, their alarm resonates with those rung during the twentieth century. Many firmly believed that the introduction of chemical and

[1] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London, UK: The International Institute for Strategic Studies, 2011).
[2] John B. Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012).
[3] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press: Potomac Books, 2009).
[4] Comment from a 6 February 2013 discussion at the School of Advanced Air and Space Studies located at Maxwell Air Force Base, Alabama.
[5] Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011), 25.

biological weapons to the battlefield would forever alter the landscape of conflict. Yet somehow, the world has managed to keep a fairly tight lid on employment of both. Despite (or perhaps because of) the overwhelming destructive power of nuclear weapons, only two have been detonated since they were first created. Determinists of the twentieth century counseled, as do those of the twenty-first, an "if you build it they will come" approach to warfare of the future, implying that once the weapon has been built, no man will stop its eventual proliferation into all of warfare. The cases of nuclear, chemical, and biological weapons as well as the ongoing work with landmines prove this need not necessarily be the case. When discrimination becomes a major factor and civilians are not just caught in the crossfire, but actively targeted by a class of weapons, existing norms of warfare have acted to constrain their use. Though not completely eliminated, their employment has become the exception rather than the rule.

Certainly, the differences in ease of proliferation between, say, nuclear and cyber weapons prevent direct correlation, but lessons from one are not wholly nontransferable to the other. Nor is it necessary to approach the geostrategic marketplace with rose-tinted glasses in order to see the prospects for an alternate future in cyberspace. International norms and regimes do not exist out of wholly altruistic feelings about the togetherness of humanity on the part of national leaders. They "why" behind such norms and regimes are often very complex and multifaceted; selfish calculations of national interests can and do play an important role in any international agreement. Rarely does a country consider a singular variable when making a national security decision. It does not matter what *truly* motivates a country to observe an international norm, only that a country *is* motivated toward compliance. By no means are countries ultimately prevented from unleashing any of these weapons if they truly desired. In the absence of a global governing body, each nation is free to act of its own accord. However, the histories of chemical, biological, and nuclear weapons as well as landmines have established precedence for and evidence of a security environment that looks very disapprovingly at civilian casualties. While this by no means guarantees a lack of cyber Armageddon, it does hint strongly that it may not be as inevitable as many would have the world believe.

Exploring the Path Less Taken

The largest problem with the current one-sided view of cyberspace is that an outsized focus on threats risks overlooking the possibility of an alternative future and therefore undercuts any effort to achieve it. With a focus on fear, the prospects for peace are undermined and cooperation is dismissed out of hand. Indeed some have gone so far as to characterize the potential for a cybersecurity treaty as a "pipe dream," insisting that national interests are better served cultivating a state of readiness and communicating distinct resolve against erstwhile cyber adversaries.[6] While peace in cyberspace may not ultimately prevail, and preparation for this prospect is certainly warranted, dismissal out of hand not only ignores lessons of the twentieth century, it sets a dangerous precedent of resignation. To surrender to the inevitability of pervasive conflict abdicates the United States of any power to shape an alternate future.

This is not a new phenomenon. "Both the threats and the opportunities presented by…new technology have a tendency to be oversold and exaggerated by its 'early adopters.' And hence there is good cause to worry that cyber power theorists are repeating an old mistake: succumbing to the 'shock of the new' where more cool-headed analysis would urge caution and more reflection on the elements of continuity than those of change."[7] No one can know today whether the forecasts of future cyber threats are over-hyped or not. As with all predictions, time remains the ultimate arbiter of truth. History, however, demonstrates that the determinist prediction of dire consequences is not assured. There remains at least some hope of an alternate future. One author cautions that determinism is an "intellectually impoverished…way to study the past, understand the present, and predict the future."[8] In exploring the landscape of future conflict, one must remember that cyberspace is a medium, not a message.[9] There is no singular setting forced upon the geopolitical stage through the mere introduction of new technologies, even those as transformative as offered by cyberspace. The world may one day experience cyber Armageddon, but its arrival is by no means a foregone conclusion.

[6] Adam Segal, and Matthew Waxman, "Why a Cybersecurity Treaty Is a Pipe Dream," (2011), http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325#.

[7] Betz and Stevens, *Cyberspace and the State*, 87.

[8] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), 290.

[9] Maj Joe "Scab" Kramer, (discussion, School of Advanced Air and Space Studies, Maxwell Air Force Base, AL, 12 February 2013).

If Armageddon is to be avoided, the existence of an alternate path must not only be acknowledged, it must be pursued.

Bibliography

Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report." *ISIS* 15 (2011).

Allison, Graham T. "Conceptual Models and the Cuban Missile Crisis." *The American Political Science Review* 63, no. 3 (1969): 689-718.

Andres, Richard B. "Strategic Cyber Offense, Cyber Defense, and Cyber Deterence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, ix, 246 p. Washington, DC: Georgetown University Press, 2012.

APT1: Exposing One of China's Cyber Espionage Units. Mandiant Report. 2013.

Armistead, Leigh. *Information Warfare: Separating Hype from Reality*. Washington, DC: Potomac Books, 2007.

Arthur D. Little. "About Us." http://www.adlittle.com/about-us.html (accessed 23 January 2013).

British Broadcasting Coroporation. "How the Web Went World Wide." http://news.bbc.co.uk/2/hi/technology/5242252.stm (accessed 24 March 2013).

Berners-Lee, Tim. "Information Management." Proposal submitted to CERN, 1989.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London, UK: The International Institute for Strategic Studies, 2011.

Bijker, Wiebe E., Thomas Parke Hughes, and T. J. Pinch. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987.

The Biological Weapons Convention. The United Nations Office at Geneva. 1972.

Bloomberg. "China Eclipses U.S. as Biggest Trading Nation." http://www.bloomberg.com/news/2013-02-09/china-passes-u-s-to-become-the-world-s-biggest-trading-nation.html (accessed 1 May 2013).

Bothe, Michael, Natalino Ronzitti, and Allan Rosas. *The New Chemical Weapons Convention--Implementation and Prospects*. The Hague ; Boston: Kluwer Law International, 1998.

Bousquet, Antoine J. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, Critical War Studies. New York: Columbia University Press, 2009.

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press, 2009.

Brodie, Bernard. *Strategy in the Missile Age*. Santa Monica, CA: RAND Corporation, 2007.

Brown, Frederic Joseph. *Chemical Warfare: A Study in Restraints*. New Brunswick, NJ: Transaction Publishers, 2006.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S. ." *The New York Times* (2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

Bunker, Robert J. "Weapons of Mass Disruption and Terrorism." *Terrorism and Political Violence* 12, no. 1 (2000): 37-46.

Bunn, George. "Gas and Germ Warfare: International Legal History and Present Status." *Proceedings of the National Academy of Sciences* 65, no. 1 (1970): 253-60.

Bunn, George. "The Nuclear Nonproliferation Treaty: History and Current Problems." *Arms Control Today* 33,no. 10 (2003), http://search.proquest.com/docview/211242485?accountid=4332.

Buono, Suzanne C. "Demystifying Nuclear Proliferation: Why States Do What They Do." PhD diss., Johns Hopkins University, 2011.

Bush, George W. President, United States of America. “Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11.” Address. United States Congress, Washington, DC, 20 September 2001.

Campen, Alan D., and Douglas H. Dearth. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. Fairfax, VA: AFCEA International Press, 2000.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: AFCEA International Press, 1996.

Casey-Maslen, Stuart. *Commentaries on Arms Control Treaties*. 2nd ed. New York: Oxford University Press, 2005.

Central Intelligence Agency. *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD*. 2004.

Cirincione, Joseph. *Bomb Scare: The History and Future of Nuclear Weapons*. New York: Columbia University Press, 2007.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2010.

Clausewitz, Carl von, Michael Howard, and Peter Paret. *On War*. Princeton, NJ: Princeton University Press, 1984.

Clinton, Hillary Rodham, United States Secretary of State. “Remarks on Internet Freedom.” Address. The Newseum, Washington, DC, 21 January 2010.

Cochran, Thomas B., William M. Arkin, Milton M. Hoenig, and Natural Resources Defense Council. *Nuclear Weapons Databook*. Cambridge, MA: Ballinger Pub. Co., 1984.

Coleman, Kim. *A History of Chemical Warfare*. New York: Palgrave Macmillan, 2005.

Craig, Campbell. *Destroying the Village: Eisenhower and Thermonuclear War*. New York: Columbia University Press, 1998.

Crimean Texts. “The Panmure Papers, Volume 1.” http://crimeantexts.russianwar.co.uk/sources/panmure/pcont08.html (accessed 22 January 2013).

Dearth, Douglas H. "Critical Infrastructures and the Human Target in Information Operations." In *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, edited by Alan D. Campen and Douglas H. Dearth, iv, 309 p. Fairfax, VA: AFCEA International Press, 2000.

Demchak, Chris C., and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (2011): 32-61.

Dilanian, Ken. "The World; Cyber-Attacks Outrank Al Qaeda as a Threat; Foreign Online Assaults Are Getting Worse, Intelligence Chiefs Say in an Annual Review." *Los Angeles Times* (2013), http://search.proquest.com/docview/1316029347?accountid=4332.

Douhet, Giulio. *The Command of the Air*. Tuscaloosa, AL: University of Alabama Press, 1998.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. *W32.Stuxnet Dossier Version 1.4 (February 2011)*: Symantec Security Response, 2011.

Fanelli, Robert, and Gregory Conti. "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict." Paper presented at the 4th International Conference on Cyber Conflict 2012.

Federal Aviation Administration. *The Economic Impact of Civil Aviation on the U.S. Economy*. 2011.

Federal Reserve Bank of San Francisco. “Ask Dr. Econ.” http://www.frbsf.org/education/activities/drecon/2012/Dr-Econ-q3.html (accessed 27 April 2013).

The Foreign Policy Initiative. “The Obama Administration's Pivot to Asia: A Conversation with Assistant Secretary Kurt Campbell, Moderated by Robert Kagan, transcript.” http://www.foreignpolicyi.org/files/uploads/images/Asia%20Pivot.pdf (accessed 20 March 2013).

Fries, Amos A., and Clarence J. West. "Chemical Warfare." New York: McGraw-Hill Book Company, inc., 1921.

Frischknecht, Friedrich. "The History of Biological Warfare." *EMBO reports* 4,no. (2003), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1326439/.

The Geneva Protocol. *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*. 1925.

Griggs, Lt Col Roy A. "Technology and Strategy." *Airpower Journal* 10,no. 2 (1996), http://www.airpower.au.af.mil/airchronicles/apj/apj96/sum96/griggs.htm.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2011.

Heinrichs, Waldo H. *Threshold of War: Franklin D. Roosevelt and American Entry into World War Ii*. New York: Oxford University Press, 1988.

Hughes, Rex. "Towards a Global Regime for Cyber Warfare." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers: Ios PressInc, 2009.

Huntington, Samuel P. "The Lonely Superpower." *Foreign Affairs* 78, no. 2 (1999): 35-49.

Ikenberry, G. John. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars*. Princeton, NJ: Princeton University Press, 2001.

Institute, Stockholm International Peace Research. *The Problem of Chemical and Biological Warfare: A Study of the Historical, Technical, Military, Legal and Political Aspects of CBW, and Possible Disarmament Measures*. Vol. 4. New York: Humanities Press, 1971.

International Campaign to Ban Landmines. *Landmine Monitor Report*. Washington, DC: Human Rights Watch, 1999.

International Campaign to Ban Landmines. *Landmine Monitor Report 2012*. 2012.

International Campaign to Ban Landmines. “Mine Ban Treaty.” http://www.icbl.org/index.php/icbl/Treaty (accessed 21 January 2013).

International Campaign to Ban Landmines. “States Not Party.” http://www.icbl.org/index.php/icbl/Universal/MBT/States-Not-Party (accessed 27 April 2013).

International Campaign to Ban Landmines. “States Parties.” http://www.icbl.org/index.php/icbl/Universal/MBT/States-Parties (accessed 21 January 2013).

The Internet Sacred Text Archive. “Hesiod: Works And Days.” http://www.sacred-texts.com/cla/hesiod/works.htm (accessed 29 January 2013).

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.

Joint Publication 5-0. *Joint Operation Planning*. 11 August 2011.

Kaku, Michio. *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100*. 1st ed. New York: Doubleday, 2011.

Kalb, Marvin. "China Is Not the Soviet Union." *Up Front* (2012), http://www.brookings.edu/blogs/up-front/posts/2012/01/10-china-kalb.

Kelly, Jack. *Gunpowder: Alchemy, Bombards, and Pyrotechnics: The History of the Explosive That Changed the World*. New York: Basic Books, 2005.

Kennedy, Paul. "The Good Old Days of the Cold War." *Los Angeles Times* (2007), http://www.latimes.com/news/la-op-kennedy18feb18,0,6800641.story.

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press, 2005.

Khong, Yuen Foong. *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965*. Princeton, NJ: Princeton University Press, 1992.

Kilcullen, David. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. Oxford ; New York: Oxford University Press, 2009.

Kramer, Joseph “Scab.” Discussion. School of Advanced Air and Space Studies, Maxwell Air Force Base, AL, 12 February 2013.

Kristensen, Hans M., and Robert S. Norris. "Russian Nuclear Forces, 2012." *Bulletin of the Atomic Scientists* 68, no. 2 (2012): 87-97.

Kristensen, Hans M., and Robert S. Norris. "US Nuclear Forces, 2012." *Bulletin of the Atomic Scientists* 68, no. 3 (2012): 84-91.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, xxii, 642 p. Washington, DC: National Defense University Press, 2009.

Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, xxii, 642 p. Washington, DC: National Defense University Press, 2009.

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. 3rd ed. Chicago, IL: University of Chicago Press, 1996.

Kurzweil, Ray. *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. New York: Viking, 1999.

Lachow, Irving. "Cyber Terrorism: Menace or Myth?" In *Cyberpower and National Security*

edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, xxii, 642 p. Washington, DC: National Defense University Press, 2009.

Lesho, Emil, David Dorsey, and David Bunner. "Feces, Dead Horses, and Fleas: Evolution of the Hostile Use of Biological Agents." *Western Journal of Medicine* 168,no. 6 (1998), http://search.proquest.com/docview/200466980?accountid=4332.

Libicki, Martin C. "Cyber Operations Can Supplement a War, but They Cannot Be the War." *The Rand Blog* (2012), http://www.rand.org/blog/2012/12/cyber-operations-can-supplement-a-war-but-they-cannot.html.

Libicki, Martin C. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8 (2012): 325-439.

Libicki, Martin C. "Military Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, xxii, 642 p. Washington, DC: National Defense University Press, 2009.

Libicki, Martin C., and Project Air Force (U.S.). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York: Frank Cass, 2004.

Matthews, Jessica T. "Power Shift." *Foreign Affairs* 76, no. 1 (1997): 50-66.

Mazetti, Mark, and David E. Sanger. "Security Leader Says U.S. Would Retaliate against Cyberattacks." *The New York Times* (2013), http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all&_r=0.

McDougall, Walter A. *The Heavens and the Earth: A Political History of the Space Age*. Baltimore, MD: Johns Hopkins University Press, 1997.

Medeiros, Evan S. *Reluctant Restraint: The Evolution of China's Nonproliferation Policies and Practices, 1980-2004*, Studies in Asian Security. Stanford, CA: Stanford University Press, 2007.

Meserve, Jeanne. "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid." *CNN.com* (2007), http://www.cnn.com/2007/US/09/26/power.at.risk/.

Miller, Roger G. *To Save a City: The Berlin Airlift, 1948-1949*. College Station, TX: Texas A&M University Press, 2000.

Minorities at Risk Project. “Chronology for Shi'is in Iraq.” http://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=country&category=&publisher=MARP&type=&coi=IRQ&rid=&docid=469f38a61e&skip=0 (accessed 28 April 2013).

Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. Tuscaloosa, AL: University of Alabama Press, 2009.

Moody, E.M. "Landmines on the Table: A Negotiations Analysis of the Global Campaign to Ban Landmines." PhD diss., University of Florida, 2008.

Morgan, Gareth. *Images of Organization*. Updated ed. Thousand Oaks, CA: Sage Publications, 2006.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs, 2011.

Mueller, John E. *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda*. New York: Oxford University Press, 2010.

The New York Times. "Search Results." http://query.nytimes.com/search/sitesearch/#/*/from20130101to20130331/ (accessed 27 April 2013).

Norris, Robert S. "Israeli Nuclear Forces, 2002." *Bulletin of the Atomic Scientists* 58, no. 5 (2002): 73.

Nye, Joseph. "Work with China, Don't Contain It." *The New York Times* (2013), http://www.nytimes.com/2013/01/26/opinion/work-with-china-dont-contain-it.html.

Organization for the Prohibition of Chemical Weapons. "Non-Member States." http://www.opcw.org/about-opcw/non-member-states/ (accessed 25 January 2013).

Organization for the Prohibition of Chemical Weapons. "OPCW Member States." http://www.opcw.org/about-opcw/member-states/ (accessed 25 January 2013).

Organization for the Prohibition of Chemical Weapons. "OPCW Statement on Alleged Chemical Weapons in Syria." http://www.opcw.org/news/article/opcw-statement-on-alleged-chemical-weapons-in-syria/ (accessed 16 April 2013).

Ottawa Landmines Convention. *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*. 1997.

Palmer, Brian. "How Dangerous Is a Cyberattack?" *Slate.com* (2012), http://www.slate.com/articles/news_and_politics/explainer/2012/04/how_dangerous_is_a_cyberattack_.html.

Pape, Robert Anthony. *Bombing to Win: Air Power and Coercion in War*. Ithaca, NY: Cornell University Press, 1996.

Paul, T.V. *Power Versus Prudence: Why Nations Forgo Nuclear Weapons*. Ithaca, NY: McGill-Queen's University Press, 2000.

Peace Treaty of Versailles. 1919.

Posen, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* 28, no. 1 (2003): 5-46.

The President of the United States. *National Security Strategy*. 2010.

Price, Richard. "A Genealogy of the Chemical Weapons Taboo." *International Organization* 49, no. 1 (1995): 73-103.

Qiao, Liang, Al Santoli, and Xiangsui Wang. *Unrestricted Warfare: China's Master Plan to Destroy America*. Panama City, Panama: Pan American Publishing, 2002.

Rafferty, Andrew. "Cybersecurity Threatens US-China Relationship, White House Official Says." *NBCNEWS.com* (2013), http://usnews.nbcnews.com/_news/2013/03/11/17273068-cybersecurity-threatens-us-china-relationship-white-house-official-says?lite.

Rathmell, Andrew. "Cyber-Terrorism: The Shape of Future Conflict?" *RUSI Journal* 142, no. 5 (1997): 40-45.

Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, xxii, 642 p. Washington, DC: National Defense University Press, 2009.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Reid, Robert W. "Diabolical in Its Simplicity, the Ancient, Durable Caltrop." *Military History* 15,no. 3 (1998), http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=841092&site=ehost-live&scope=site&custid=airuniv.

Reiss, Mitchell. *Bridled Ambition: Why Countries Constrain Their Nuclear Capabilities*. Washington, DC: Johns Hopkins University Press, 1995.

Reveron, Derek S. "An Introduction to National Security and Cyberspace." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, ix, 246 p. Washington, DC: Georgetown University Press, 2012.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2011): 5-32.

Rothkopf, David. "The Enemy Within." *Foreign Policy*, no. 193 (2012): 1-3.

Roy, R., and S. Friesen. "Historical Uses of Antipersonnel Landmines: Impact on Land Force Operations." *Department of National Defense Canada* (1999): 2-36.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. 1st ed. New York: Crown Publishers, 2012.

Sanger, David E. "In Cyberspace, New Cold War." *The New York Times* (2013), http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.

Schneck, William C. "The Origins of Military Mines: Part I." *Engineer* 28,no. 3 (1998), http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=1123648&site=ehost-live&scope=site&custid=airuniv.

Segal, Adam, and Matthew Waxman. "Why a Cybersecurity Treaty Is a Pipe Dream." (2011), http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325#.

Shachtman, Noah. "Russia’s Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals." *Wired* (2012), http://www.wired.com/dangerroom/2012/07/ff_kaspersky/all/.

Shackelford, Scott James. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27,no. 1 (2009), http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7/.

Sheldon, John B. "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, ix, 246 p. Washington, DC: Georgetown University Press, 2012.

Sidell, Frederick R., Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, Textbook of Military Medicine Part I, Warfare, Weaponry, and the Casualty. Washington, DC: Borden Institute, 1997.

Singer, P.W. "A Defense Policy Vision." *Armed Forces Journal* (June 2011), http://www.armedforcesjournal.com/2011/06/6462790.

Smith, Merritt Roe, and Leo Marx. *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, MA: MIT Press, 1994.

Starr, Stuart H. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, xxii, 642 p. Washington, DC: National Defense University Press: Potomac Books, 2009.

Stephenson, Charles. *The Admiral's Secret Weapon: Lord Dundonald and the Origins of Chemical Warfare*. Rochester, NY: Boydell, 2006.

Thakur, Ramesh Chandra, Ere Haru, and United Nations University. *The Chemical Weapons Convention: Implementation, Challenges and Opportunities*. New York: United Nations University Press, 2006.

Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." *Parameters* 26, no. 4 (1996): 81-91.

Tucker, Jonathan B. "Evidence Iraq Used Chemical Weapons During the 1991 Persian Gulf War." *The Nonproliferation Review* 4, no. 3 (1997): 114-22.

Tzu, Sun. *The Illustrated Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 2005.

Waldman, Carl. *Atlas of the North American Indian*. 3rd ed. New York: Facts on File, 2009.

The United Nations Office at Geneva. “Membership of the Biological Weapons Convention.” http://www.unog.ch/80256EE600585943/(httpPages)/7BE6CBBEA0477B52C12571860035FD5C?OpenDocument (accessed 22 January 2013).

United Nations Office for Disarmament Affairs. “Treaty on the Non-Proliferation of Nuclear Weapons.” http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml (accessed 16 April 2013).

United States Environmental Protection Agency. *Transportation Modal Shares of World Trade and U.S. Trade with the World, 2008*. 2008.

United States Government Accountability Office. *Freight Railroads: Industry Health Has Improved, but Concerns About Competition and Capacity Should Be Addressed*. 2006.

Wegener, Henning. "Harnessing the Perils in Cyberspace: Who Is in Charge?" Paper presented at the Disarmament Forum, 2007.

Wendt, Alexander. *Social Theory of International Politics*, Cambridge Studies in International Relations. New York: Cambridge University Press, 1999.

West, Clarence J. "Chemical Warfare." Cambridge, MA: Arthur D. Little, inc., 1919.

West, Clarence J. "The History of Poison Gases." *Science* 49, no. 1270 (1919): 412-17.

Wheelis, Mark. "Biological Warfare at the 1346 Siege of Caffa." *Emerging Infectious Diseases* 8,no. 9 (2002), http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=7433556&site=ehost-live&scope=site&custid=airuniv.

White, Lynn Townsend. *Medieval Technology and Social Change*. Oxford, UK: Clarendon Press, 1962.

Yale Law School. “Laws of War: Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases; July 29, 1899.” http://avalon.law.yale.edu/19th_century/dec99-02.asp (accessed 22 January 2013).

Youngblood, Norman. *The Development of Mine Warfare: A Most Murderous and Barbarous Conduct*, War, Technology, and History,. Westport, CT: Praeger Security International, 2006.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Threat Level* (2011), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/.